UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
15/752,711	02/14/2018	Nick Armstrong	AMK-5243-9

CONFIRMATION NO. 5327

POA ACCEPTANCE LETTER

162809
Bochner IP, PLLC
295 Madison Avenue
12th Floor
New York, NY 10017

OC000000135454479

Date Mailed: 07/29/2022

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 07/21/2022.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/sstephanos/

JPMC Ex. 1002
Page 1

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82A (07-13)
Approved for use through 03/31/2021. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	15/752,711
Filing Date	2018-02-14
First Named Inventor	Nick Armstrong
Title	COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR
Art Unit	3692
Examiner Name	AMANULLA ABDULLAEV
Attorney Docket Number	AMK-5243-9

SIGNATURE of Applicant or Patent Practitioner

Signature	/Andrew D. Bochner/	Date (Optional)	
Name	Andrew D. Bochner	Registration Number	68,189
Title (if Applicant is a juristic entity)			
Applicant Name (if Applicant is a juristic entity)			

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

*Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82B (07-13)
Approved for use through 03/31/2021. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)

☑ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above: 162809

OR

I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

Please recognize or change the correspondence address for the application identified in the attached transmittal letter or the boxes above to:

☑ The address associated with the above-mentioned Customer Number

OR

The address associated with Customer Number:

OR

Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

Identitii Ltd

Inventor or Joint Inventor (title not required below)

Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)

☑ Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)

Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature		Date (Optional)	8 June 2022
Name	John Rayment		
Title	CEO		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

Total of forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/96 (08-12)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: Identitii Pty Ltd

Application No./Patent No.: 10,984,413 Filed/Issue Date: 2021-04-20

Titled: COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR

Identitii Pty Ltd, a Corporation

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☑ The assignee of the entire right, title, and interest.

2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):

   ☐ The extent (by percentage) of its ownership interest is _____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.

   ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (*e.g.*, bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

A. ☑ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel 045034, Frame 0789, or for which a copy thereof is attached.

B. ☐ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

   1. From: _____ To: _____

      The document was recorded in the United States Patent and Trademark Office at

      Reel _____, Frame _____, or for which a copy thereof is attached.

   2. From: _____ To: _____

      The document was recorded in the United States Patent and Trademark Office at

      Reel _____, Frame _____, or for which a copy thereof is attached.

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450**.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/96 (08-12)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☐ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Andrew D Bochner/	2022-07-19
Signature	Date
Andrew D. Bochner	68,189
Printed or Typed Name	Title or Registration Number

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	46221175
Application Number:	15752711
International Application Number:	
Confirmation Number:	5327
Title of Invention:	COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR
First Named Inventor/Applicant Name:	Nick Armstrong
Customer Number:	23117
Filer:	Andrew David Bochner/Eugenia Baek
Filer Authorized By:	Andrew David Bochner
Attorney Docket Number:	AMK-5243-9
Receipt Date:	21-JUL-2022
Filing Date:	14-FEB-2018
Time Stamp:	12:57:15
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	1256-002US-POA.pdf	166546 06cdce58793dc307312e02de0acc102f8571a716	no	2

Warnings:

Information:					
2	Assignee showing of ownership per 37 CFR 3.73	1256-002US-3-73CFR.pdf	190538 d311c8994c46e6187b29b60168a75ddfdfe5a814	no	3
Warnings:					
Information:					
		Total Files Size (in bytes):	357084		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/752,711	04/20/2021	10984413	AMK-5243-9	5327

23117 7590 03/31/2021

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 197 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Identitii Pty Ltd, Surry Hills, New South Wales, AUSTRALIA;
Nick Armstrong, Sydney, AUSTRALIA;
Ben Buckingham, Sydney, AUSTRALIA;
Daniel Friedman, Sydney, AUSTRALIA;
Elliot Shepherd, Sydney, AUSTRALIA;
Eric Knight, Sydney, AUSTRALIA;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

23117 7590 12/02/2020
NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/752,711	02/14/2018	Nick Armstrong	AMK-5243-9	5327

TITLE OF INVENTION: COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$600	$0.00	$0.00	$600	03/02/2021

EXAMINER	ART UNIT	CLASS-SUBCLASS
ABDULLAEV, AMANULLA	3692	705-039000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 NIXON & VANDERHYE P.C.
2
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: IDENTITII PTY LTD

(B) RESIDENCE: (CITY and STATE OR COUNTRY): SURRY HILLS, NEW SOUTH WALES, AUSTRALIA

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. Fees submitted: ☒ Issue Fee ☐ Publication Fee (if required) ☐ Advance Order - # of Copies _____

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

☒ Electronic Payment via EFS-Web ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)

☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. 14-1140

5. **Change in Entity Status** (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

☐ Applicant asserting small entity status. See 37 CFR 1.27

☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /Alan M. Kagen/ Date March 1, 2021

Typed or printed name Alan M. Kagen Registration No. 36,178

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:	Conf. No.: 5327
ARMSTRONG et al.	Atty. Ref.: AMK-5243-0009
Application No.: 15/752,711	Art Unit: 3692
Filed: 02/14/2018	Examiner: ABDULLAEV, AMANULLA

For: COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR

March 1, 2021

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

COMMENTS ON EXAMINER'S STATEMENT OF REASONS FOR ALLOWANCE

With respect to the Examiner's Statement of Reasons for Allowance in the Notice of Allowance dated December 2, 2020, Applicants respectfully disagree with the Examiner to any extent that such statement characterizes the invention in a manner at variance with the actual wording of the claims. In this context, the Statement paraphrases features defined in the claims. For example, the Statement refers to "requesting generation of a token corresponding to the financial transaction to identify the documents." Claim 59, however, defines "one or more" documents pertaining to the financial transaction. Further language from the claims is similarly paraphrased. Additionally, Applicants do not concede the Examiner's characterizations of the prior art; rather, the references speak for themselves.

As set forth in the Notice of Allowance, these comments are being filed along with the payment of the Issue Fee.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: /Alan M. Kagen/
Alan M. Kagen
Reg. No. 36,178

AMK:jls
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100

Electronic Patent Application Fee Transmittal

Application Number:	15752711
Filing Date:	14-Feb-2018
Title of Invention:	COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR
First Named Inventor/Applicant Name:	Nick Armstrong
Filer:	Alan Mark Kagen/Janet Stoy
Attorney Docket Number:	AMK-5243-9

Filed as Small Entity

Filing Fees for U.S. National Stage under 35 USC 371

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
UTILITY APPL ISSUE FEE	2501	1	600	600

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**600**

Electronic Acknowledgement Receipt

EFS ID:	42053550
Application Number:	15752711
International Application Number:	
Confirmation Number:	5327
Title of Invention:	COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR
First Named Inventor/Applicant Name:	Nick Armstrong
Customer Number:	23117
Filer:	Alan Mark Kagen/Janet Stoy
Filer Authorized By:	Alan Mark Kagen
Attorney Docket Number:	AMK-5243-9
Receipt Date:	01-MAR-2021
Filing Date:	14-FEB-2018
Time Stamp:	15:26:41
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$600
RAM confirmation Number	E202131F26540317
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	5243-9_issue_fee.pdf	101495 87f0a7b10c8a5c0e64a3655065021c5584b1d1d7	no	1
Warnings:					
Information:					
2	Post Allowance Communication - Incoming	5243-9_comments_on_allowance.pdf	19439 cedbf88c1d8d9b9f0b310d60cc6e3aea181584b4	no	1
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30590 99e9ad5d4a89ba376904e531b4758a1be065e411	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	151524		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	Conf. No.: 5327
ARMSTRONG et al.	Atty. Ref.: AMK-5243-0009
Appln. No. 15/752,711	Art Unit: 3692
Filed: 02/14/2018	Examiner: ABDULLAEV, AMANULLA

For: COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR

* * * * * * * * * * *

February 10, 2021

Mail Stop Issue Fee
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

RULE 312 AMENDMENT

In response to the Notice to File Corrected Application Papers dated January 7, 2021, pursuant to 37 C.F.R. § 1.312, please amend the above-identified patent application as follows:

Amendments to the Drawings begin on page 2.

Remarks/Arguments begin on page 3.

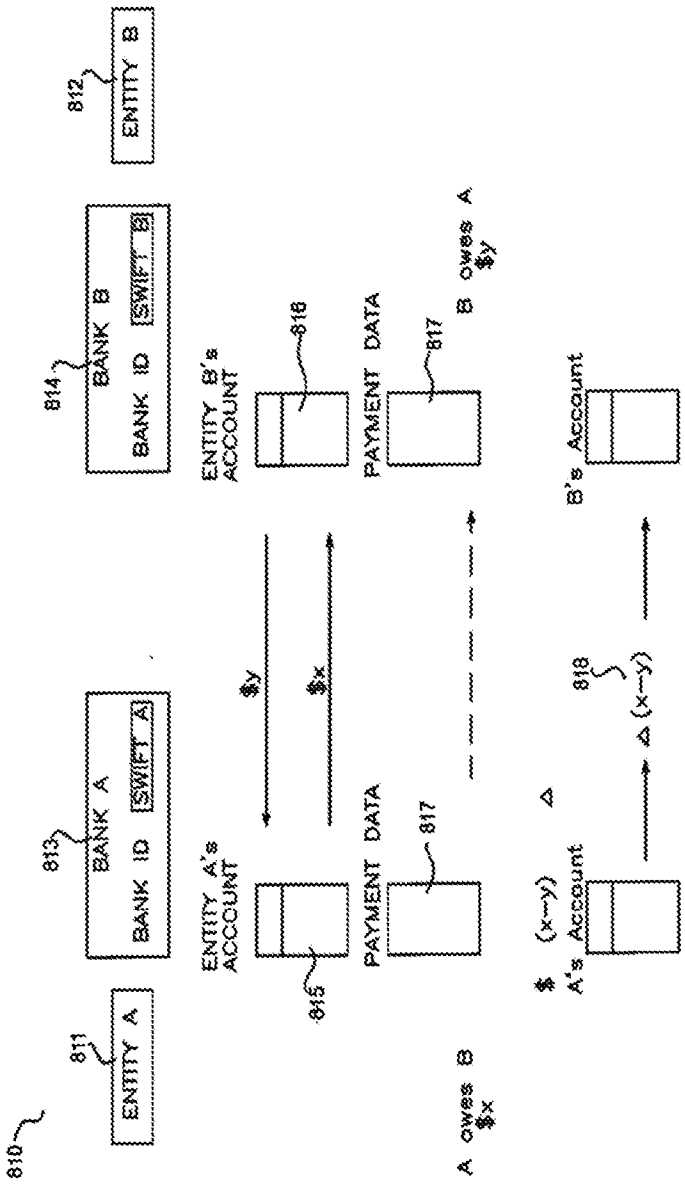


FIG. 8A
[PRIOR ART]

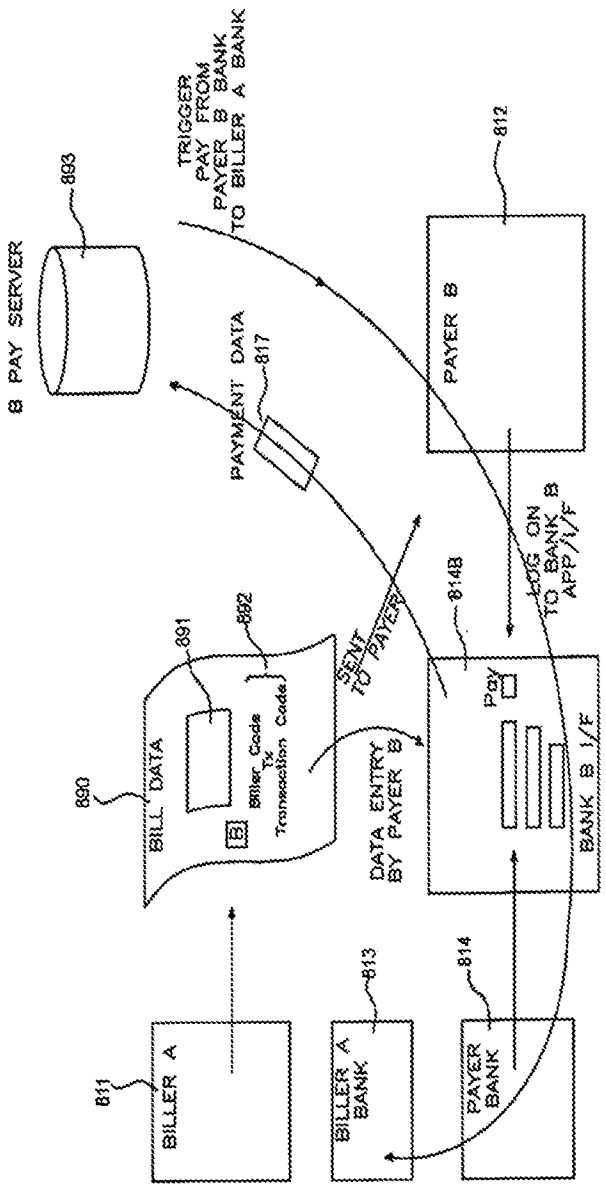


FIG. 8B
[PRIOR ART]

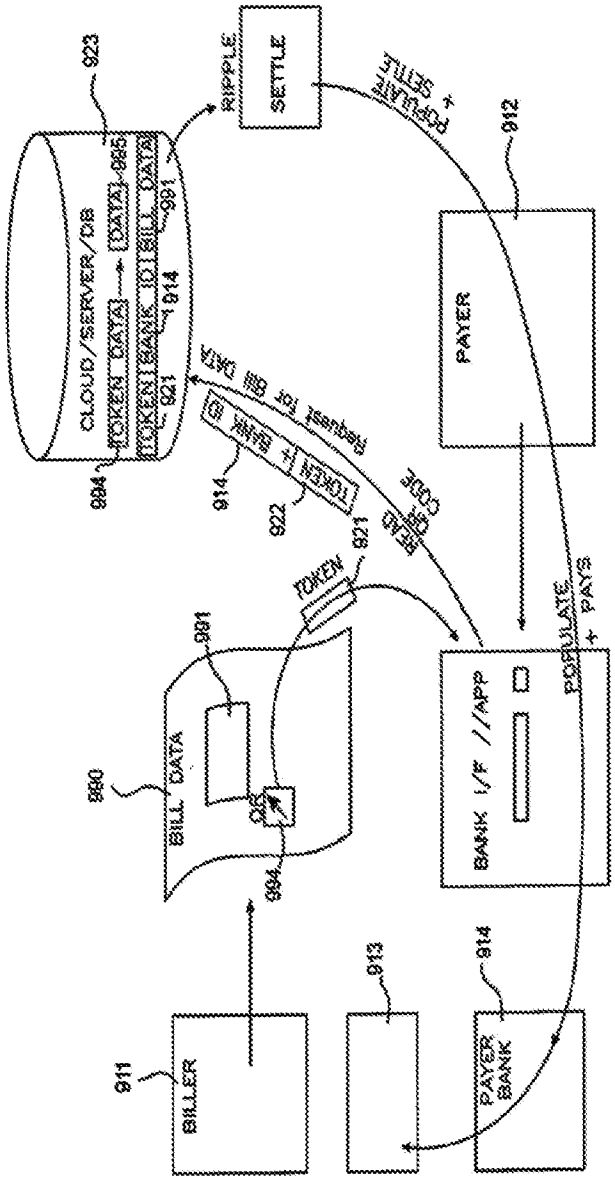

923
RIPPLE
SETTLE
912
PAYER
CLOUD/SERVER/DB
[DATA]-995
991
BILL DATA
914
921
914
922
921
TOKEN
991
990
BILL DATA
995
994
BANK I/F //APP
911
BILLER
913
914
PAYER BANK

FIG. 9A

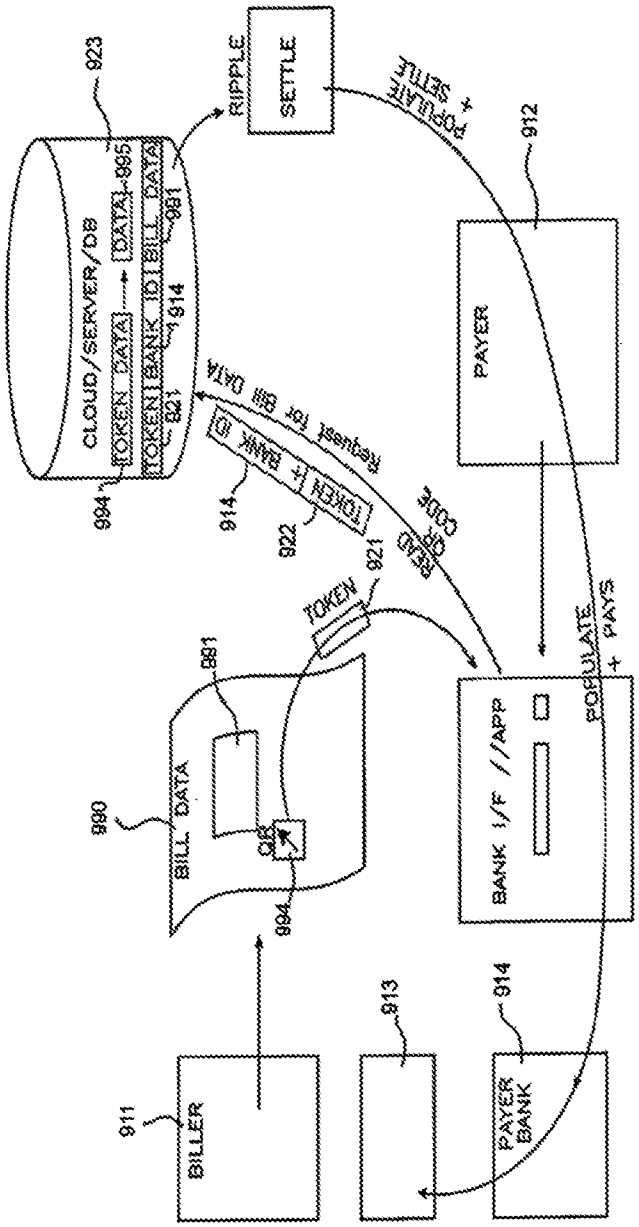

923
RIPPLE
SETTLE
912
CLOUD/SERVER/DB
[TOKEN DATA]
[DATA]-995
[TOKEN] BANK ID] BILL DATA
981
914
821
994
914
922
921
TOKEN
881
990
BILL DATA
QR
994
BANK I/F //APP
PAYER
911
BILLER
913
914
PAYER BANK

FIG. 9B

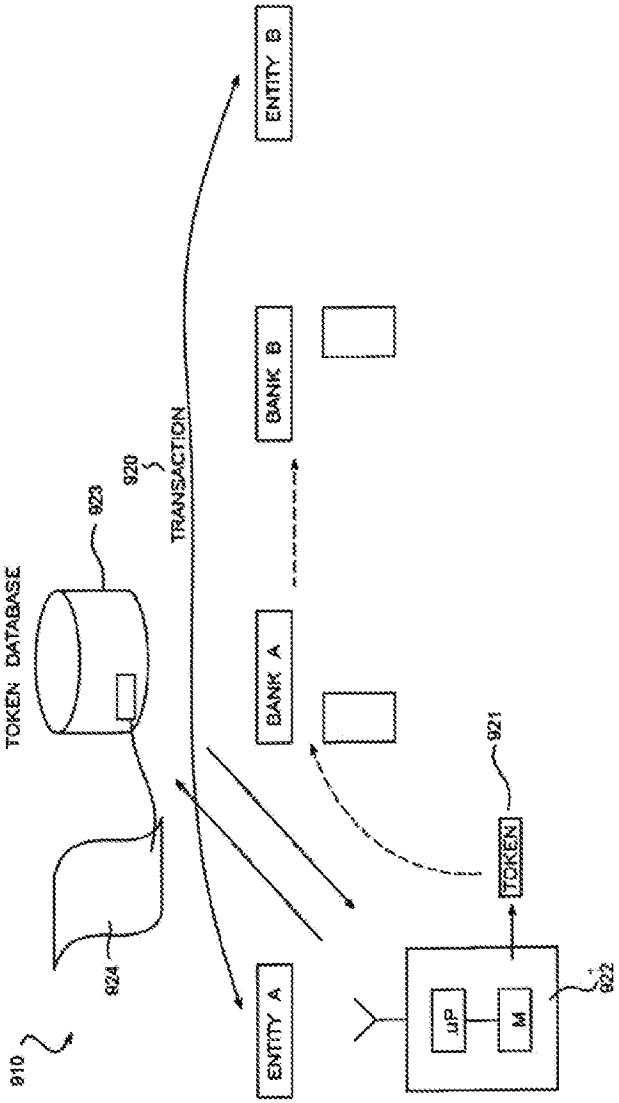

ENTITY B
BANK B
BANK A
ENTITY A
TRANSACTION
920
923
TOKEN DATABASE
924
910
921
TOKEN
922
uP
M

FIG. 9C

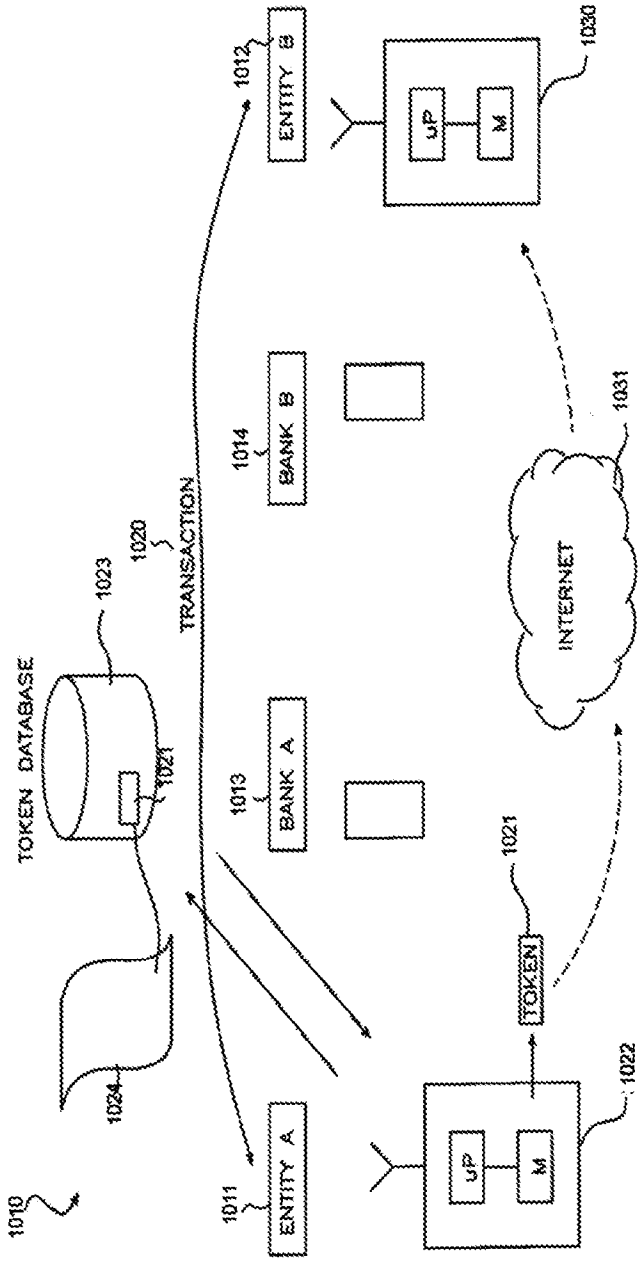

1010
1011
ENTITY A
1012
ENTITY B
1013
BANK A
1014
BANK B
1020
TRANSACTION
1021
TOKEN
1022
uP
M
1023
TOKEN DATABASE
1024
1030
1031
INTERNET

FIG. 10A

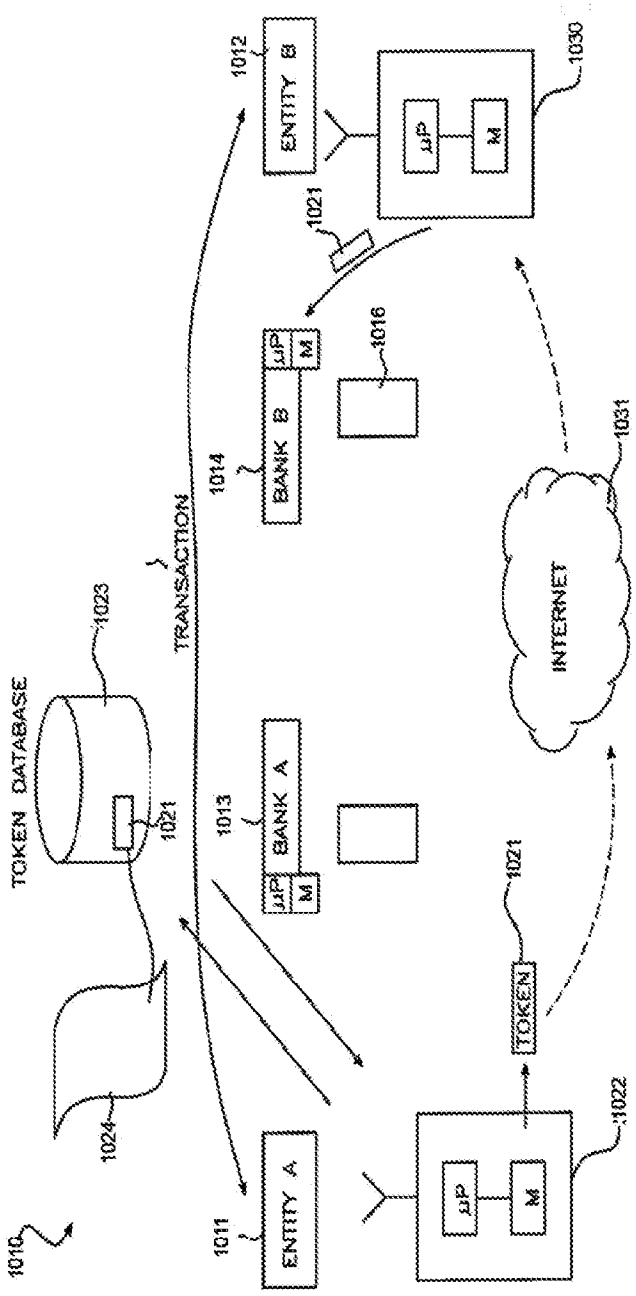

1010
1011
ENTITY A
1012
ENTITY B
1013
BANK A
1014
BANK B
1016
1021
1022
1023
1024
1030
1031
TOKEN DATABASE
TRANSACTION
INTERNET
TOKEN
μP
M

FIG. 10B

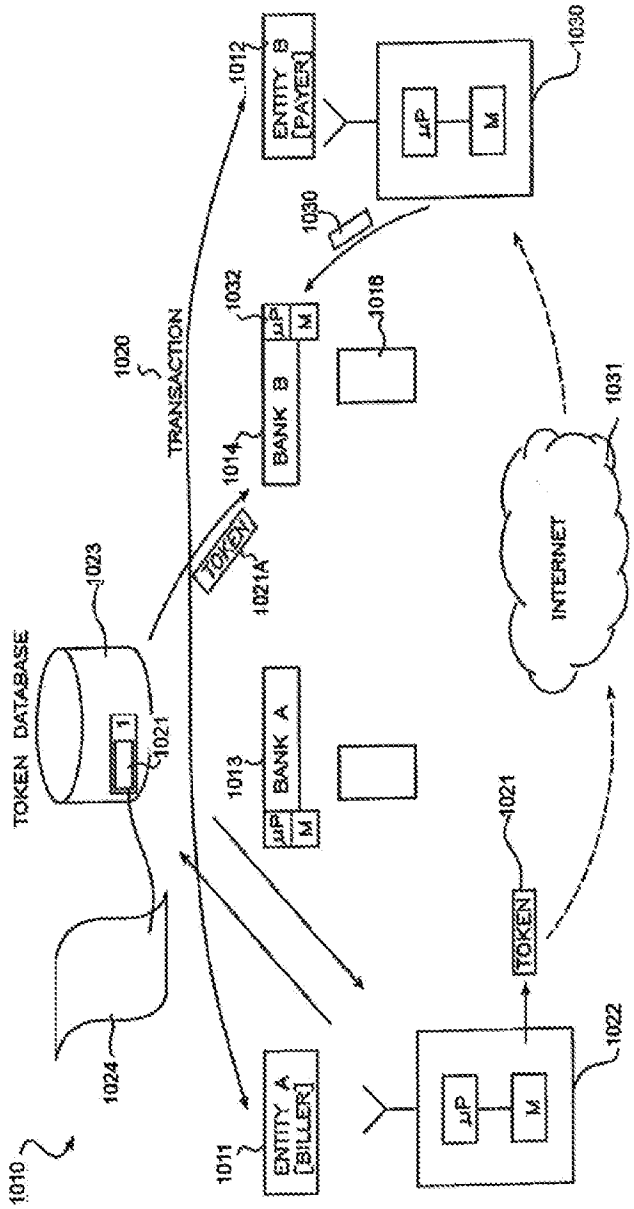

1010
1011
ENTITY A [BILLER]
1012
ENTITY B [PAYER]
1013
BANK A
1014
BANK B
1018
1020
TRANSACTION
1021
1021A
1022
1023
1024
1030
1031
INTERNET
1032
TOKEN
TOKEN DATABASE
μP
M

FIG. 10C

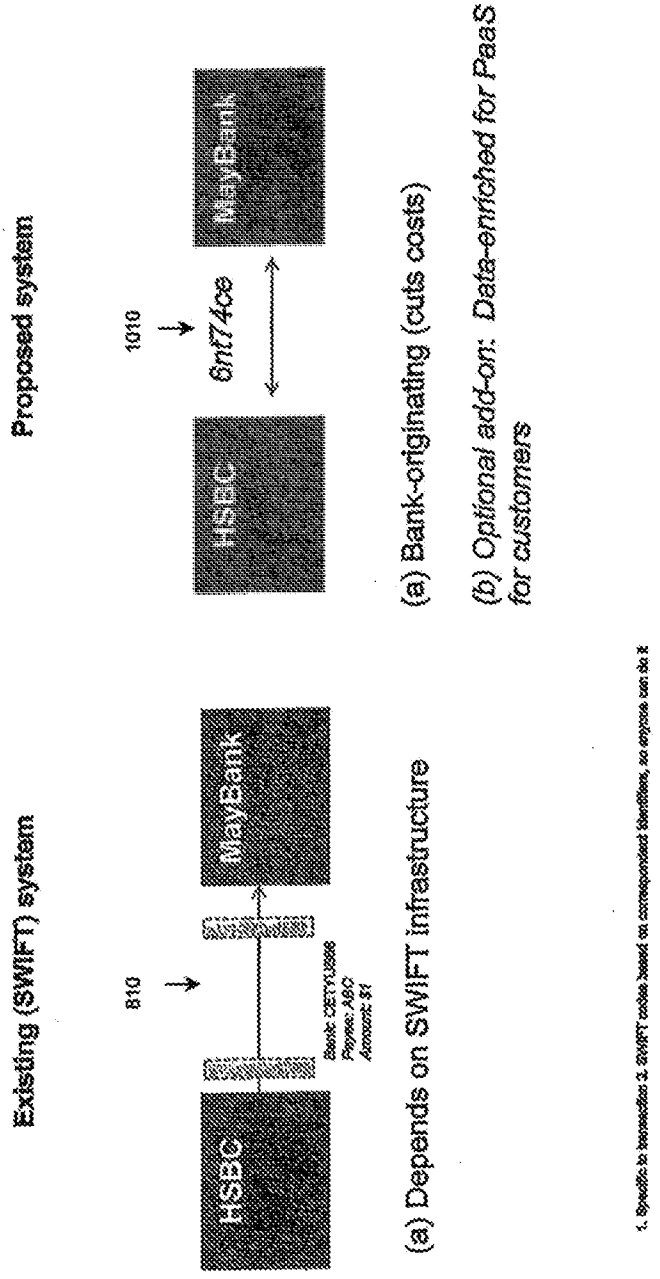

Existing (SWIFT) system
Proposed system
HSBC
MayBank
810
1010
6nf74ce
(a) Depends on SWIFT infrastructure
(a) Bank-originating (cuts costs)
(b) Optional add-on: Data-enriched for PaaS for customers

FIG. 11

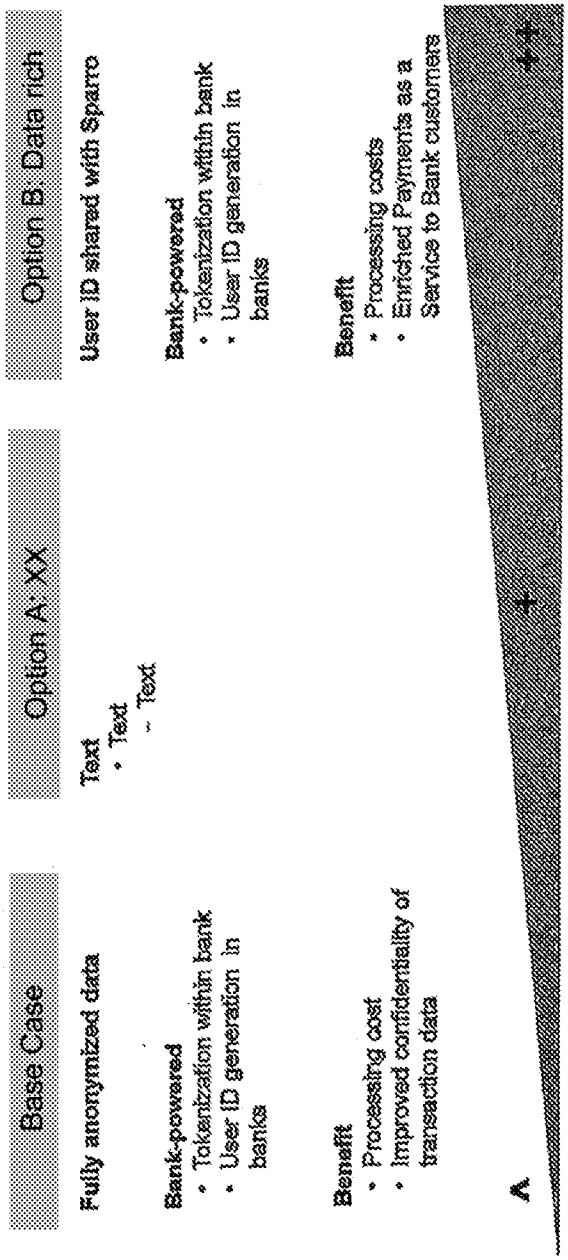

Base Case
Option A: XX
Option B: Data rich
Fully anonymized data
Text
• Text
- Text
User ID shared with Sparro
Bank-powered
• Tokenization within bank
• User ID generation in banks
Bank-powered
• Tokenization within bank
• User ID generation in banks
Benefit
• Processing cost
• Improved confidentiality of transaction data
Benefit
• Processing costs
• Enriched Payments as a Service to Bank customers
+
++

FIG. 12

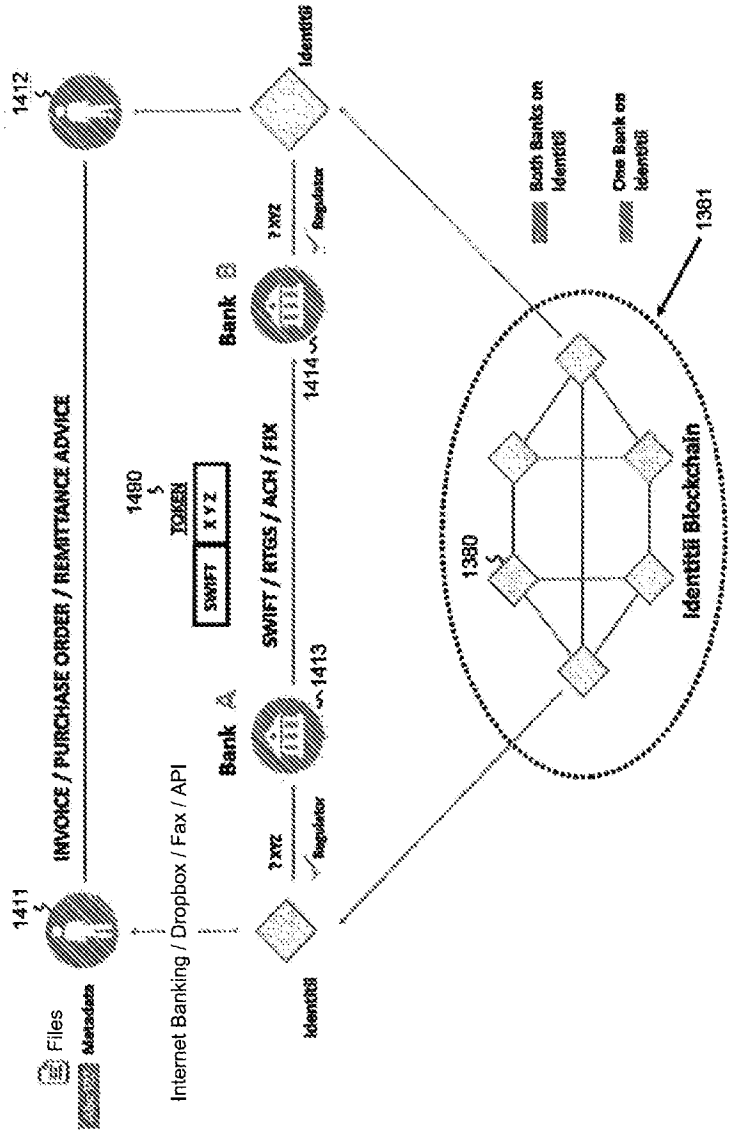

1412
1411
INVOICE / PURCHASE ORDER / REMITTANCE ADVICE
Files
Metadata
Internet Banking / Dropbox / Fax / API
1480
TOKEN
XYZ
SWIFT
Bank
Bank
SWIFT / RTGS / ACH / FIX
1414
1413
Regulator
Regulator
Both Banks on Identiti
One Bank on Identiti
1381
1380
Identiti Blockchain

FIG. 14

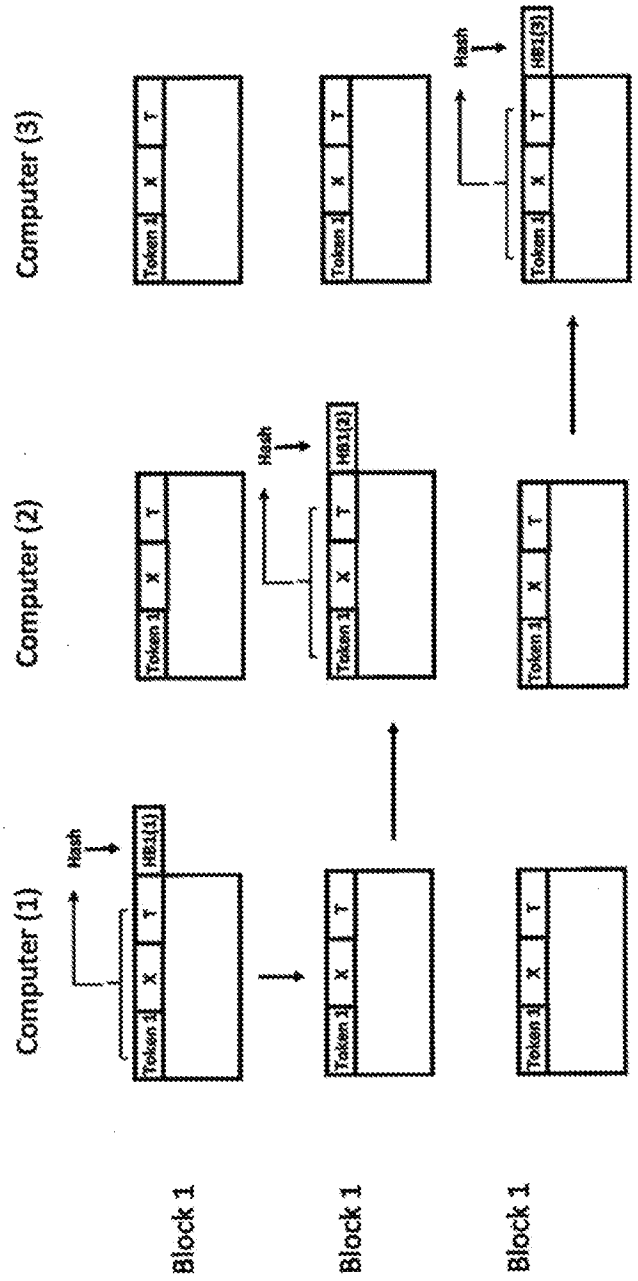

Computer (3)
Computer (2)
Computer (1)
Hash
Token 1
X
T
HB1(1)
HB1(2)
HB1(3)
Block 1
Block 1
Block 1

FIG. 15B

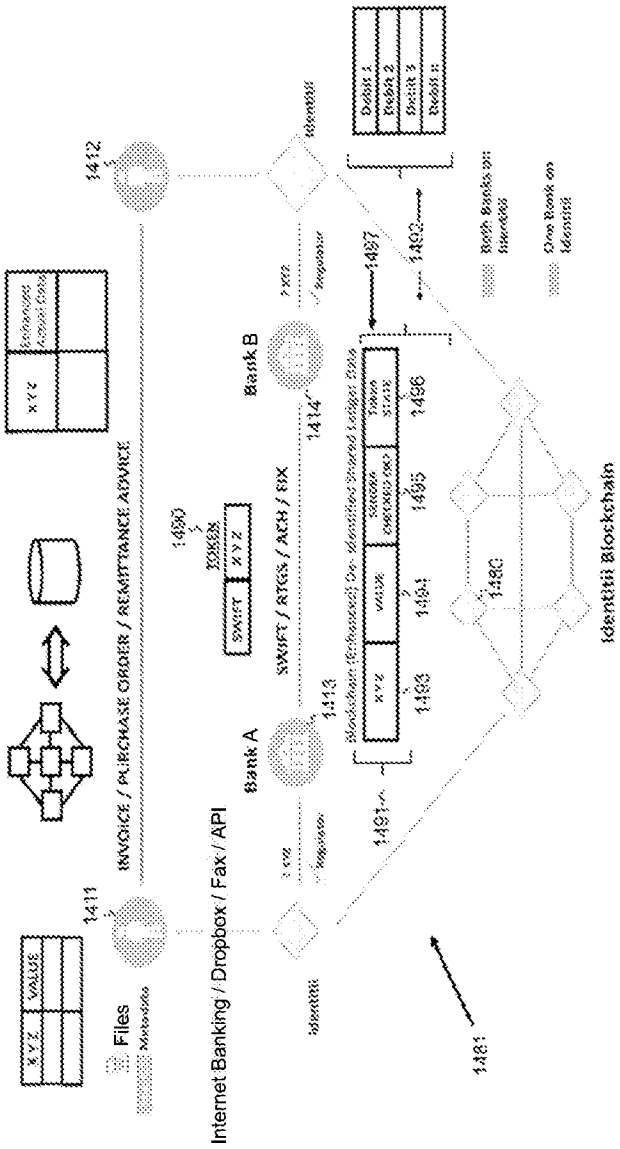

1411
1412
Files
INVOICE / PURCHASE ORDER / REMITTANCE ADVICE
Internet Banking / Dropbox / Fax / API
Bank A
Bank B
SWIFT / RTGS / ACH / FIX
1414
1416
1418
1481
1482
1486
1487
1491
1493
1494
1495
1496
Identity Blockchain

FIG. 16

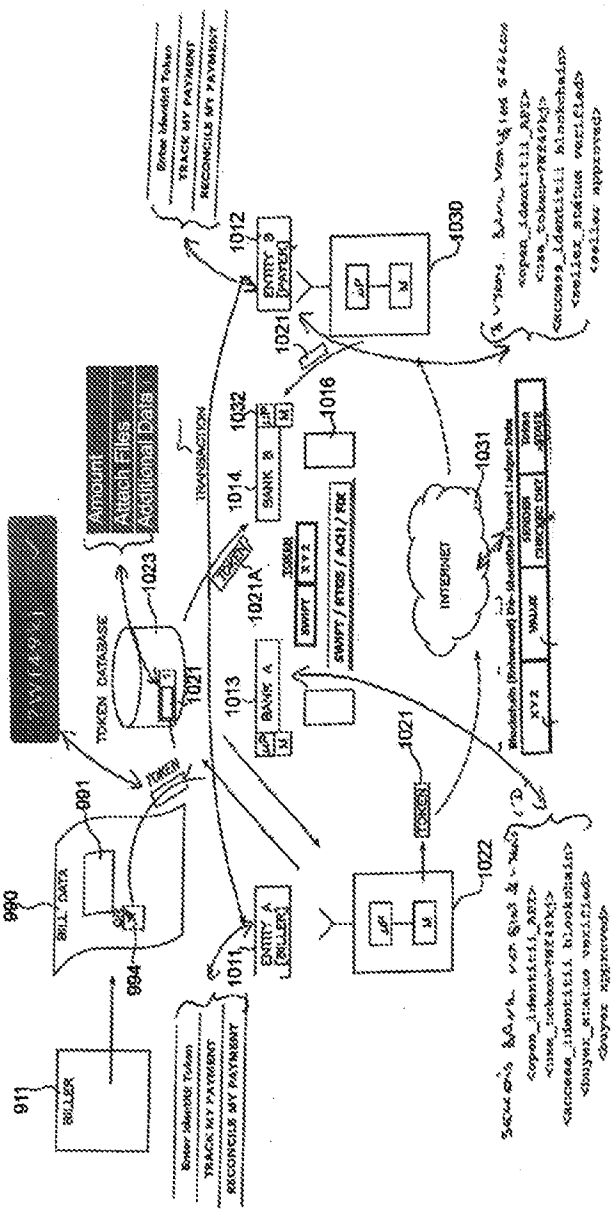

990
991
994
911
BILLER
BILL DATA
1011
1012
1013
1014
1016
1021
1021A
1022
1023
1030
1031
1032
TOKEN DATABASE
TOKEN
TRANSACTION
INTERNET
SWIFT / RTGS / ACH / RTP

FIG. 17

Electronic Acknowledgement Receipt

EFS ID:	41885069
Application Number:	15752711
International Application Number:	
Confirmation Number:	5327
Title of Invention:	COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR
First Named Inventor/Applicant Name:	Nick Armstrong
Customer Number:	23117
Filer:	Alan Mark Kagen/Janet Stoy
Filer Authorized By:	Alan Mark Kagen
Attorney Docket Number:	AMK-5243-9
Receipt Date:	10-FEB-2021
Filing Date:	14-FEB-2018
Time Stamp:	09:54:01
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		5243-9_rule_312_amd_and_copy_of_notice.pdf	1178901 ff77773ebca7aa864930d0651834fa126df49ca6	yes	6

	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Amendment after Notice of Allowance (Rule 312)		1	1	
	Applicant Arguments/Remarks Made in an Amendment		2	6	
Warnings:					
Information:					
2	Drawings-only black and white line drawings	5243-9_replacement_sheets_of_drawings.pdf	4763253 8b9cc686a535f5552506d0a5c83f37830fa52783	no	14
Warnings:					
Information:					
		Total Files Size (in bytes):	5942154		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

AMENDMENTS TO THE DRAWINGS

The attached sheets of drawings include changes to Figs. 8A-12, 14 and 15B-17. These sheets, which include Figs. 8A-12, 14 and 15B-17, replace the original sheets including Figs. 8A-12, 14 and 15B-17. The Figures have been revised to address the drawing objections in the Notice.

Attachment: Replacement Sheets

3072206 JPMC Ex. 1002
Page 33

REMARKS/ARGUMENTS

The drawings were objected to in a Notice to File Corrected Application Papers. Figs. 8A-12, 14 and 15B-17 have been revised to improve the character of the lines, numbers, and letters in the noted figures. Withdrawal of the objection is requested.

Applicants submit that this Amendment under 37 CFR 1.312 raises no new issues, and entry of the amendment is respectfully requested.

The Commissioner is hereby authorized to charge any deficiency, or credit any overpayment, in the fee(s) filed, or asserted to be filed, or which should have been filed herewith (or with any paper hereafter filed in this application by this firm) to Deposit Account No. 14-1140.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: /Alan M. Kagen/
Alan M. Kagen
Reg. No. 36,178

AMK:jls
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/752,711	02/14/2018	Nick Armstrong	AMK-5243-9	5327

23117 7590 01/07/2021
NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER
ABDULLAEV, AMANULLA

ART UNIT	PAPER NUMBER
3692	

NOTIFICATION DATE	DELIVERY MODE
01/07/2021	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTOMAIL@nixonvan.com
pair_nixon@firsttofile.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

Application No. : 15752711
Applicant : Armstrong
Filing Date : 02/14/2018
Date Mailed : 01/07/2021

NOTICE TO FILE CORRECTED APPLICATION PAPERS

Notice of Allowance Mailed

This application has been accorded an Allowance Date and is being prepared for issuance. The application, however, is incomplete for the reasons below.

Applicant is given two (2) months from the mail date of this Notice within which to respond. This time period for reply is extendable under 37 CFR 1.136(a) for only TWO additional MONTHS.

The informalities requiring correction are indicated in the attachment(s). If the informality pertains to the abstract, specification (including claims) or drawings, the informality must be corrected with an amendment in compliance with 37 CFR 1.121 (or, if the application is a reissue application, 37 CFR 1.173). Such an amendment may be filed after payment of the issue fee if limited to correction of informalities noted herein. See Waiver of 37 CFR 1.312 for Documents Required by the Office of Patent Publication, 1280 Off. Gaz. Patent Office 918 (March 23, 2004). In addition, if the informality is not corrected until after payment of the issue fee, for purposes of 35 U.S.C. 154(b)(1)(iv), "all outstanding requirements" will be considered to have been satisfied when the informality has been corrected. A failure to respond within the above-identified time period will result in the application being ABANDONED.

See attachment(s).

A copy of this notice MUST be returned with the reply. Please address response to "Mail Stop Issue Fee, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450".

/Kam Sin/
Publication Branch
Office of Data Management
(571) 272-4200

IDENTIFICATION OF DRAWING DEFICIENCIES

- [ ] There is a hole or the image thereof within the illustration. FIG(s)
- [ ] The illustration is penetrated or traversed by a solid or broken line that is not intended to be part of the drawing, such as a dark line caused by a flaw in the copying process. FIG(s)
- [ ] An ink stamp or the image thereof obscures part of the illustration. FIG(s)
- [ ] The drawing is marred by black smudges, obliterations, or fax/copier marks (for example, speckles or dots in a substantial portion of the drawing). FIG(s)
- [ ] Figure numbers are duplicated or missing. FIG(s)
- [ ] Drawing sheet or figure is missing. FIG(s)
- [ ] Numbers, letters, or reference characters in the drawing have been crossed out or are illegibly handwritten. FIG(s)
- [X] The character of the lines, numbers, and letters is poor. FIG(s) 8A-12, 14, 15B-17
- [ ] The drawing's background shows that the original drawing was made on graph paper or other paper with a pattern or decoration. FIG(s)
- [ ] The FIG. number label is placed in a location that causes the drawing to be read upside down. FIG(s)
- [ ] Data, a reference number, or part of the drawing is truncated or missing, or a lead line has no reference number. FIG(s)
- [ ] The drawing and/or the FIG. label contain(s) foreign language. FIG(s)
- [ ] This utility application contains a photograph of a view that is capable of being illustrated as a line drawing. FIG(s)
- [ ] A petition under 37 CFR 1.84(a)(2) to accept color drawings has been granted, but the brief description of the drawings in the specification does not contain (or has not been amended to contain) the paragraph required by 37 CFR 1.84(a)(2)(iii).
- [ ] This reissue application contains added and/or amended drawings that are not labeled as "New" or "Amended" or "Canceled" as required by 37 CFR 1.173(b)(3). FIG(s)
- [ ] This Design reissue application contains a drawing that is labeled as "Canceled" but is not surrounded by brackets, or a drawing that is surrounded by brackets but is not labeled as "Canceled." See 37 CFR 1.173(b)(3). FIG(s)
- [ ] OTHER:
- [ ] COMMENTS:

SCORE Placeholder Sheet for IFW Content

Application Number: 15752711 Document Date: 02/10/2021

The presence of this form in the IFW record indicates that the following document type was received in electronic format on the date identified above. This content is stored in the SCORE database.

Since this was an electronic submission, there is no physical artifact folder, no artifact folder is recorded in PALM, and no paper documents or physical media exist. The TIFF images in the IFW record were created from the original documents that are stored in SCORE.

- Drawing

At the time of document entry (noted above):

- USPTO employees may access SCORE content via DAV or via the SCORE web page.
- External customers may access SCORE content via PAIR using the Supplemental Content tab.

Form Revision Date: March 1, 2019

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/752,711	02/14/2018	Nick Armstrong	AMK-5243-9	5327

23117 7590 01/11/2021

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
ABDULLAEV, AMANULLA	

ART UNIT	PAPER NUMBER
3692	

NOTIFICATION DATE	DELIVERY MODE
01/11/2021	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTOMAIL@nixonvan.com
pair_nixon@firsttofile.com

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR/ PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
15/752,711	02/14/2018	Armstrong et al.	AMK-5243-9

		EXAMINER	
NIXON & VANDERHYE, PC 901 NORTH GLEBE ROAD, 11TH FLOOR ARLINGTON, VA 22203		AMANULLA ABDULLAEV	
		ART UNIT	PAPER
		3692	20201228

DATE MAILED: _____

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

37 CFR 1.96 Submission of computer program listings.
(b) Material which will be printed in the patent: If the computer program listing is contained in 300 lines or fewer, with each line of 72 characters or fewer, it may be submitted either as drawings or as part of the specification.
(2) Specification.
(i) If the listing is submitted as part of the specification, it must be submitted in accordance with the provisions of § 1.52.
(ii) Any listing having more than 60 lines of code that is submitted as part of the specification must be positioned at the end of the description but before the claims. Any amendment must be made by way of submission of a substitute sheet.
(c) As an appendix which will not be printed: Any computer program listing may, and any computer program listing having over 300 lines (up to 72 characters per line) must, be submitted on a compact disc in compliance with § 1.52(e). A compact disc containing such a computer program listing is to be referred to as a "computer program listing appendix." The "computer program listing appendix" will not be part of the printed patent. The specification must include a reference to the "computer program listing appendix" at the location indicated in § 1.77(b)(5).

The application should be in compliance with the mentioned above provisions.

During the phone call on December 29, 2020 the Applicant affirmed that a compliant specification will be submitted. And said application is on file as of 1/5/2021.

/AMANULLA ABDULLAEV/ Examiner, Art Unit 3692	/BRUCE I EBERSMAN/ Primary Examiner, Art Unit 3692

PTO-90C (Rev.04-03)

Response to Rule 312 Communication	Application No.	Applicant(s)	
	15/752,711	Armstrong, Nick	
	Examiner	Art Unit	AIA (FITF) Status
	BRUCE I EBERSMAN	3692	Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

1. ☑ The amendment filed on 05 January 2021 under 37 CFR 1.312 has been considered, and has been:

a) ☐ entered.

b) ☑ entered as directed to matters of form not affecting the scope of the invention.

c) ☐ disapproved because the amendment was filed after the payment of the issue fee.

Any amendment filed after the date the issue fee is paid must be accompanied by a petition under 37 CFR 1.313(c)(1) and the required fee to withdraw the application from issue.

d) ☐ disapproved. See explanation below.

e) ☐ entered in part. See explanation below.

/BRUCE I EBERSMAN/
Primary Examiner, Art Unit 3692

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/752,711	02/14/2018	Nick Armstrong	AMK-5243-9	5327

23117 7590 01/07/2021
NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER
ABDULLAEV, AMANULLA

ART UNIT	PAPER NUMBER
3692	

NOTIFICATION DATE	DELIVERY MODE
01/07/2021	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTOMAIL@nixonvan.com
pair_nixon@firsttofile.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

Application No. : 15752711
Applicant : Armstrong
Filing Date : 02/14/2018
Date Mailed : 01/07/2021

NOTICE TO FILE CORRECTED APPLICATION PAPERS

Notice of Allowance Mailed

This application has been accorded an Allowance Date and is being prepared for issuance. The application, however, is incomplete for the reasons below.

Applicant is given two (2) months from the mail date of this Notice within which to respond. This time period for reply is extendable under 37 CFR 1.136(a) for only TWO additional MONTHS.

The informalities requiring correction are indicated in the attachment(s). If the informality pertains to the abstract, specification (including claims) or drawings, the informality must be corrected with an amendment in compliance with 37 CFR 1.121 (or, if the application is a reissue application, 37 CFR 1.173). Such an amendment may be filed after payment of the issue fee if limited to correction of informalities noted herein. See Waiver of 37 CFR 1.312 for Documents Required by the Office of Patent Publication, 1280 Off. Gaz. Patent Office 918 (March 23, 2004). In addition, if the informality is not corrected until after payment of the issue fee, for purposes of 35 U.S.C. 154(b)(1)(iv), "all outstanding requirements" will be considered to have been satisfied when the informality has been corrected. A failure to respond within the above-identified time period will result in the application being ABANDONED.

See attachment(s).

A copy of this notice MUST be returned with the reply. Please address response to "Mail Stop Issue Fee, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450".

/Kam Sin/
Publication Branch
Office of Data Management
(571) 272-4200

IDENTIFICATION OF DRAWING DEFICIENCIES

- [ ] There is a hole or the image thereof within the illustration. FIG(s)
- [ ] The illustration is penetrated or traversed by a solid or broken line that is not intended to be part of the drawing, such as a dark line caused by a flaw in the copying process. FIG(s)
- [ ] An ink stamp or the image thereof obscures part of the illustration. FIG(s)
- [ ] The drawing is marred by black smudges, obliterations, or fax/copier marks (for example, speckles or dots in a substantial portion of the drawing). FIG(s)
- [ ] Figure numbers are duplicated or missing. FIG(s)
- [ ] Drawing sheet or figure is missing. FIG(s)
- [ ] Numbers, letters, or reference characters in the drawing have been crossed out or are illegibly handwritten. FIG(s)
- [X] The character of the lines, numbers, and letters is poor. FIG(s) 8A-12, 14, 15B-17
- [ ] The drawing's background shows that the original drawing was made on graph paper or other paper with a pattern or decoration. FIG(s)
- [ ] The FIG. number label is placed in a location that causes the drawing to be read upside down. FIG(s)
- [ ] Data, a reference number, or part of the drawing is truncated or missing, or a lead line has no reference number. FIG(s)
- [ ] The drawing and/or the FIG. label contain(s) foreign language. FIG(s)
- [ ] This utility application contains a photograph of a view that is capable of being illustrated as a line drawing. FIG(s)
- [ ] A petition under 37 CFR 1.84(a)(2) to accept color drawings has been granted, but the brief description of the drawings in the specification does not contain (or has not been amended to contain) the paragraph required by 37 CFR 1.84(a)(2)(iii).
- [ ] This reissue application contains added and/or amended drawings that are not labeled as "New" or "Amended" or "Canceled" as required by 37 CFR 1.173(b)(3). FIG(s)
- [ ] This Design reissue application contains a drawing that is labeled as "Canceled" but is not surrounded by brackets, or a drawing that is surrounded by brackets but is not labeled as "Canceled." See 37 CFR 1.173(b)(3). FIG(s)
- [ ] OTHER:
- [ ] COMMENTS:

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	Atty. Ref.: AMK-5243-0009
ARMSTRONG et al.	Confirmation No. 5327
Appl. No. 15/752,711	Art Unit: 3692
Filed: 02/14/2018	Examiner: ABDULLAEV, AMANULLA

For: COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR

* * * * * * * * * * *

MAIL STOP ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

January 5, 2021

Sir:

AMENDMENT UNDER 37 CFR § 1.312

In response to the Notice of Allowance dated December 2, 2020, pursuant to 37 C.F.R. §1.312, please amend the above-identified application as follows:

Amendments to the Specification begin on page 2.

Remarks/Arguments begin on page 3.

JPMC Ex. 1002
Page 45

AMENDMENTS TO THE SPECIFICATION:

Please DELETE the specification in its entirety in favor of the attached substitute specification. A marked-up copy of the substitute specification showing all changes relative to the immediate prior version of the specification of record is attached. Applicant submits that no new matter has been added to the specification.

JPMC Ex. 1002
Page 46

REMARKS/ARGUMENTS

By this Amendment under 37 C.F.R. 1.312, the specification has been amended as requested by the Examiner. Specifically, according to 37 C.F.R. 1.96, the computer program listing, which is contained in less than 300 lines, with 72 characters or fewer per line, has been positioned at the end of the description but before the claims. See 37 C.F.R. 1.96(b)(2) and MPEP §608.05(a).

A version of the specification with markings showing all the changes relative to the immediate prior version of the specification of record is included along with an accompanying clean version (without markings). See 37 C.F.R. 1.125. Applicants submit that the substitute specification includes no new matter. In the substitute specification, paragraphs [0164]-[0402] have been positioned at the end of the description but before the claims.

Entry is respectfully requested.

The Commissioner is hereby authorized to charge any deficiency, or credit any overpayment, in the fee(s) filed, or asserted to be filed, or which should have been filed herewith (or with any paper hereafter filed in this application by this firm) to Deposit Account No. 14-1140.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: /Alan M. Kagen/
Alan M. Kagen
Reg. No. 36,178

AMK:jls
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100

JPMC Ex. 1002
Page 47

COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR

[001] This application is the U.S. national phase of International Application No. PCT/AU2016/000279 filed August 12, 2016 which designated the U.S. and claims priority to Australian Patent Application No. 2015903292 filed August 14, 2015, Australian Patent Application No. 2016900239 filed January 27, 2016, and Australian Patent Application No. 2016901924 filed May 20, 2016, the entire contents of each of which are hereby incorporated by reference.

Field of the Invention

[002] The present invention relates to financial transactions and in particular to a method and a system for processing a financial transaction.

[003] The invention has been developed primarily for use in/with financial transactions and will be described hereinafter with reference to this application. However, it will be appreciated that the invention is not limited to this particular field of use.

Background of the Invention

[004] A financial transaction comprises at least two parties, with a transfer of currency taking place between the two parties. The currency may include electronic currency and fiat currency. In either case, any financial transaction includes a plurality of data associated with the financial transaction. The plurality of data may include payment metadata such as account numbers of the at least two parties, Business Identifier Codes (BIC) of the financial institutions corresponding to the at least two parties, amount of currency to be transferred and type of currency etc. Further, the plurality of data may include regulatory compliance documents such as KYC documents.

JPMC Ex. 1002
Page 48

[005] Generally, it is difficult to keep track of the plurality of data during the financial transaction. Further, it is even more difficult to ensure that integrity of the plurality of data is maintained either during or after the financial transaction has been completed or to evidence that it existed at a certain point in the financial transaction process. Many settlement systems are characterised by effective one-way transmission of the plurality of data in any given financial transaction (for example systems based on SWIFT messaging). If it is subsequently discovered that there are deficiencies in the plurality of data transmitted, time consuming checking and querying operations and correspondence often ensues before the financial transaction can be effected.

[006] Therefore there remains, in the art, a need for improved methods and systems for processing a financial transaction which do not suffer from the above mentioned issues.

[007] Any discussion of the background art throughout the specification should in no way be considered as an admission that such background art is prior art, nor that such background art is widely known or forms part of the common general knowledge in the field in Australia or any other country.

Summary of the Invention

[008] According to a first aspect of the present invention, there is provided a computer implemented method for processing a financial transaction, the method comprising the steps of transmitting one or more documents pertaining to the financial transaction, from a first intermediary server to a first document store, generating an enriched data record from the one or more documents, at the first intermediary server, and adding the enriched data record into a blockchain, from the first intermediary sever, requesting generation of a token corresponding to the financial transaction, to a token server, from the first intermediary server, via a messaging bus, generating

JPMC Ex. 1002
Page 49

the token at the token server and adding the token into the blockchain from the token server, transmitting the token to the first intermediary server from the token server, via the messaging bus and transmitting the token from the first intermediary server to the first document store. The token provides a pointer to the enriched data record in the blockchain. Thus the token can used to retrieve the enriched data record at a time of an audit.

[009] In one embodiment of the invention, the computer implemented method further comprises the step of sending a first financial message comprising the token, from the first intermediary server to a second intermediary server, indicative of making a payment to a second user.

[010] In one embodiment of the invention, the computer implemented method further comprises the steps of implementing a smart contract at the token server; and adding the smart contract into the blockchain, from the token server.

[011] In one embodiment of the invention, the computer implemented method further comprises the steps of transmitting the token from the first intermediary server to a first digital device available with a first user, providing the token to a second user, by the first user, providing the token to a second intermediary server, from the second digital device, transmitting the token to a second document store, from the second intermediary server and sending a second financial message comprising the token, from the second intermediary server to the first intermediary server, indicative of making a payment to the first user.

[012] In one embodiment of the invention, the step of generating the enriched data record comprises extracting a plurality of attributes from the one or more documents, at the first intermediary server and combining the plurality

of attributes to generate the enriched data record, at the first intermediary server.

[013] In one embodiment of the invention, the step of generating the enriched data record comprises extracting a plurality of attributes from the one or more documents, at the first intermediary server, de-identifying the plurality of attributes to obtain a plurality of de-identified attributes, at the first intermediary server and combining the plurality of de-identified attributes to generate the enriched data record, at the first intermediary server. De-identification of the plurality of attributes ensures that confidentiality of any person or entity involved in the financial transaction is not compromised during a hacking attack on the blockchain.

[014] In one embodiment of the invention, the step of generating the enriched data record comprises extracting a plurality of attributes from the one or more documents, at the first intermediary server, hashing the plurality of attributes to generate a plurality of respective hashes, at the first intermediary server and combining the plurality of hashes to generate the enriched data record, at the first intermediary server. Hashing provides even more protection against tampering of theft, to the one or more documents, as the hashes are irreversible.

[015] In one embodiment of the invention, the computer implemented method further comprises the step of assigning a payment risk rating to the token. The payment risk rating is a direct measure of the regulatory and other compliance checks involved in the financial transaction.

[016] In one embodiment of the invention, the computer implemented method further comprises the steps of transmitting one or more first requests, each comprising the token, from the first intermediary server to the second

intermediary server, via the messaging bus, receiving the one or more first requests at the second intermediary server and transmitting the one or more first requests and the token from the second intermediary server to a second document store, generating one or more first responses, each comprising the token, corresponding to the respective one or more first requests, at the second intermediary server, transmitting the one or more first responses from the second intermediary server to the first intermediary server, via the messaging bus, hashing the one or more first requests and the one or more first responses at the second intermediary server to generate one or more first request hashes and one or more first response hashes, respectively, adding the one or more first request hashes and the one or more first response hashes to the enriched data record in the blockchain, from the second intermediary server and receiving the one or more first responses at the first intermediary server and transmitting the one or more first responses to the first document store. This communication between the first intermediary server and the second intermediary server allows the first intermediary server to execute all the necessary compliance checks.

[017] In one embodiment of the invention, the computer implemented method further comprises the steps of hashing the one or more first responses at the first intermediary server to regenerate the one or more first response hashes and verifying the one or more first response hashes with the blockchain from the first intermediary server, using the token. Thus, the integrity of the one or more first responses can be verified with the blockchain, at any given time.

[018] In one embodiment of the invention, each one of the one or more first requests are encrypted with a second public key and signed with a first public key at the first intermediary server, before transmission to the second intermediary server and decrypted with a second private key at the second

JPMC Ex. 1002
Page 52

intermediary server after reception from the first intermediary server. Further, each one of the one or more first responses are encrypted with the first public key and signed with the second public key at the second intermediary server, before transmission to the first intermediary server and decrypted with a first private key at the first intermediary server after reception from the second intermediary server. Using pairs of asymmetrical keys ensures that the requests and the responses are not intercepted during transmission.

[019] In one embodiment of the invention, the one or more first responses comprise one or more second regulatory compliance documents pertaining to a second user.

[020] In one embodiment of the invention, the computer implemented method further comprises the steps of transmitting one or more second requests, each comprising the token, from the second intermediary server to the first intermediary server, via the messaging bus, receiving the one or more second requests at the first intermediary server and transmitting the one or more second requests from the first intermediary server to the first document store, generating one or more second responses, each comprising the token, corresponding to the respective one or more second requests, at the first intermediary server, transmitting the one or more second responses from the first intermediary server to the second intermediary server, via the messaging bus, hashing the one or more second requests and the one or more second responses at the first intermediary server to generate one or more second request hashes and one or more second response hashes, respectively, adding the one or more second request hashes and the one or more second response hashes to the enriched data record in the blockchain, from the first intermediary server and receiving the one or more second responses at the second intermediary

server and transmitting the one or more second responses to the second document store. This communication enables the second intermediary server to execute all the necessary compliance checks.

[021] In one embodiment of the invention, the computer implemented method further comprises the steps of hashing the one or more second responses at the second intermediary server to regenerate the one or more second response hashes and verifying the one or more second response hashes with the blockchain from the second intermediary server, using the token. Similar to one or more first responses, the integrity of the one or more second responses can be verified with the blockchain, at any given time.

[022] In one embodiment of the invention, each one of the one or more second requests are encrypted with a first public key and signed with a second public key at the second intermediary server, before transmission to the first intermediary server and decrypted with a first private key at the first intermediary server after reception from the second intermediary server. Further, each one of the one or more second responses are encrypted with the second public key and signed with the first public key at the first intermediary server, before transmission to the second intermediary server and decrypted with a second private key at the second intermediary server after reception from the first intermediary server. Using pairs of asymmetrical keys ensures that the requests and the responses are not intercepted during transmission.

[023] In one embodiment of the invention, the computer implemented method further comprises the steps of adding the first public key from the first intermediary server into the blockchain and adding the second public key from the second intermediary server into the blockchain.

[024] In one embodiment of the invention, the one or more second responses comprise one or more first regulatory compliance documents pertaining to a first user.

[025] According to a second aspect of the present invention, there is provided a system for processing a financial transaction, the system comprising a first intermediary server operably connected to a network and a first document store, a token server operably connected to the network, a messaging bus operably connected to the network and a blockchain operably connected to the network. Further, the first intermediary server is configured to transmit one or more documents pertaining to the financial transaction, to the first document store, generate an enriched data record from the one or more documents and add the enriched data record into the blockchain, request generation of a token corresponding to the financial transaction, to the token server, via the messaging bus and transmit the token to the first document store. Further, the token server is configured to generate the token and add the token into the blockchain and transmit the token to the first intermediary server, via the messaging bus.

[026] In one embodiment of the invention, the system further comprises a second intermediary server operably connected to the network and a second document store. Further, the first intermediary server is further configured to send a first financial message comprising the token, to the second intermediary server, indicative of making a payment to a second user.

[027] In one embodiment of the invention, the token server is further configured to implement a smart contract and add the smart contract into the blockchain.

[028] In one embodiment of the invention, the system further comprises a first digital device operably connected to the network, a second digital device operably connected to the network, a second intermediary server operably connected to the network and a second document store. Further, the first intermediary server is further configured to transmit the token to the first digital device. Further, the first digital device comprises a first memory and a first processor operably connected to the first memory, the first memory comprising a first computer program code, the first computer program code when executed by the first processor, instructs the first processor to receive the token from the first intermediary server, provide the token to the second digital device. Further, the second digital device comprises a second memory and a second processor operably connected to the second memory, the second memory comprising a second computer program code, the second computer program code when executed by the second processor, instructs the second processor to receive the token from the first digital device and provide the token to the second intermediary server. Also, the second intermediary server is configured to receive the token from the second digital device, transmit the token to the second document store and send a second financial message comprising the token, to the first intermediary server, indicative of making a payment to a first user.

[029] In one embodiment of the invention, for generation of the enriched data record, the first intermediary server is configured to extract a plurality of attributes from the one or more documents and combine the plurality of attributes to generate the enriched data record.

[030] In one embodiment of the invention, for generation of the enriched data record, the first intermediary server is configured to extract a plurality of attributes from the one or more documents, de-identify the plurality of

attributes to obtain a plurality of de-identified attributes and combine the plurality of de-identified attributes to generate the enriched data record.

[031] In one embodiment of the invention, for generation of the enriched data record, the first intermediary server is configured to extract a plurality of attributes from the one or more documents, hash the plurality of attributes to generate a plurality of respective hashes and combine the plurality of hashes to generate the enriched data record.

[032] In one embodiment of the invention, the first intermediary server is further configured to assign a payment risk rating to the token.

[033] In one embodiment of the invention, the system further comprises a second intermediary server operably connected to the network and a second document store. Further, the first intermediary server is configured to transmit one or more first requests, each comprising the token, to the second intermediary server, via the messaging bus and receive one or more first responses and transmit the one or more first responses to the first document store. Further, the second intermediary server is configured to receive the one or more first requests from the first intermediary server and transmit the one or more first requests and the token to the second document store, generate the one or more first responses, each comprising the token, corresponding to the respective one or more first requests, transmit the one or more first responses to the first intermediary server, via the messaging bus, hash the one or more first requests and the one or more first responses to generate one or more first request hashes and one or more first response hashes, respectively and add the one or more first request hashes and the one or more first response hashes to the enriched data record in the blockchain.

[034] In one embodiment of the invention, the first intermediary server is further configured to hash the one or more first responses to regenerate the one or more first response hashes and verify the one or more first response hashes with the blockchain, using the token.

[035] In one embodiment of the invention, the first intermediary server is further configured to encrypt each one of the one or more first requests with a second public key and sign each one of the one or more first requests with a first public key, before transmission to the second intermediary server and decrypt each one of the one or more first responses with a first private key after reception from the second intermediary server. Further, the second intermediary server is further configured to encrypt the each one of the one or more first responses with the first public key and sign the each one of the one or more first responses with the second public key, before transmission to the first intermediary server and decrypt the each one of the one or more first requests with a second private key after reception from the first intermediary server.

[036] In one embodiment of the invention, the one or more first responses comprise one or more second regulatory compliance documents pertaining to a second user.

[037] In one embodiment of the invention, the system further comprises a second intermediary server connected to the network and a second document store. Further, the second intermediary server is configured to transmit one or more second requests, each comprising the token, to the first intermediary server, via the messaging bus, receive one or more second responses and transmit the one or more second responses to the second document store. Further, the first intermediary server is further configured to receive the one or more second requests and transmit the one

or more second requests to the first document store, generate the one or more second responses, each comprising the token, corresponding to the respective one or more second requests, transmit the one or more second responses to the second intermediary server, via the messaging bus, hash the one or more second requests and the one or more second responses to generate one or more second request hashes and one or more second response hashes, respectively and add the one or more second request hashes and the one or more second response hashes to the enriched data record in the blockchain.

[038] In one embodiment of the invention, the second intermediary server is further configured to hash the one or more second responses to regenerate the one or more second response hashes and verify the one or more second response hashes with the blockchain, using the token.

[039] In one embodiment of the invention, the second intermediary server is further configured to encrypt each one of the one or more second requests with a first public key and sign each one of the one or more second requests with a second public key, before transmission to the first intermediary server and decrypt each one of the one or more second responses with a second private key after reception from the first intermediary server. Further, the first intermediary server is further configured to encrypt the each one of the one or more second responses with the second public key and sign the each one of the one or more second responses with the first public key, before transmission to the second intermediary server and decrypt the each one of the one or more second requests with a first private key after reception from the second intermediary server.

[040] In one embodiment of the invention, the first intermediary server is further configured to add the first public key into the blockchain and the

second intermediary server is further configured to add the second public key into the blockchain.

[041] In one embodiment of the invention, the one or more second responses comprise one or more first regulatory compliance documents pertaining to a first user.

[042] According to a third aspect of the present invention, there is provided a token server for facilitating processing of a financial transaction, operably connected to a network and configured to generate a token, add the token into a blockchain and transmit the token to a first intermediary server, via a messaging bus.

[043] In one embodiment of the invention, the token server is further configured to implement a smart contract and add the smart contract into the blockchain.

[044] According to a fourth aspect of the present invention, there is provided a first intermediary server for facilitating processing of a financial transaction, operably connected to a network and a first document store, and configured to transmit one or more documents pertaining to the financial transaction, to the first document store, generate an enriched data record from the one or more documents and add the enriched data record into a blockchain, request generation of a token corresponding to the financial transaction, to a token server, via a messaging bus and transmit the token to the first document store.

[045] In one embodiment of the invention, the first intermediary server is further configured to send a first financial message comprising the token, to

a second intermediary server, indicative of making a payment to a second user.

[046] In one embodiment of the invention, the first intermediary server is further configured to transmit the token to a first digital device.

[047] In one embodiment of the invention, for generation of the enriched data record, the first intermediary server is configured to extract a plurality of attributes from the one or more documents and combine the plurality of attributes to generate the enriched data record.

[048] In one embodiment of the invention, for generation of the enriched data record, the first intermediary server is configured extract a plurality of attributes from the one or more documents, de-identify the plurality of attributes to obtain a plurality of de-identified attributes and combine the plurality of de-identified attributes to generate the enriched data record.

[049] In one embodiment of the invention, for generation of the enriched data record, the first intermediary server is configured to extract a plurality of attributes from the one or more documents, hash the plurality of attributes to generate a plurality of respective hashes and combine the plurality of hashes to generate the enriched data record.

[050] In one embodiment of the invention, the first intermediary server is further configured to assign a payment risk rating to the token.

[051] In one embodiment of the invention, the first intermediary server is further configured to transmit one or more first requests, each comprising the token, to a second intermediary server, via the messaging bus and

receive one or more first responses from the second intermediary server and transmit the one or more first responses to the first document store.

[052] In one embodiment of the invention, the one or more first responses comprise one or more second regulatory compliance documents pertaining to a second user.

[053] In one embodiment of the invention, the first intermediary server is further configured to hash the one or more first responses to regenerate one or more first response hashes and verify the one or more first response hashes with the blockchain, using the token.

[054] In one embodiment of the invention, the first intermediary server is further configured to encrypt each one of the one or more first requests with a second public key and sign each one of the one or more first requests with a first public key, before transmission to the second intermediary server and decrypt each one of the one or more first responses with a first private key after reception from the second intermediary server.

[055] In one embodiment of the invention, the first intermediary server is further configured to receive the one or more second requests from a second intermediary server and transmit the one or more second requests to the first document store, generate one or more second responses, each comprising the token, corresponding to the respective one or more second requests, transmit the one or more second responses to the second intermediary server, via the messaging bus, hash the one or more second requests and the one or more second responses to generate one or more second request hashes and one or more second response hashes, respectively and add the one or more second request hashes and the one

or more second response hashes to the enriched data record in the blockchain.

[056] In one embodiment of the invention, the first intermediary server is further configured to encrypt each one of the one or more second responses with a second public key and sign the each one of the one or more second responses with a first public key, before transmission to the second intermediary server and decrypt each one of the one or more second requests with a first private key after reception from the second intermediary server.

[057] In one embodiment of the invention, the first intermediary server is further configured to add the first public key into the blockchain.

[058] According to a fifth aspect of the present invention, there is provided a second intermediary server for facilitating processing of a financial transaction, operably connected to a network and a second document store, and configured to receive the token from the second digital device, transmit the token to the second document store and send a second financial message comprising the token to a first intermediary server, indicative of making a payment to a first user.

[059] According to a sixth aspect of the present invention, there is provided a second intermediary server for facilitating processing of a financial transaction, operably connected to a network and a second document store, and configured to receive one or more first requests, each comprising a token, from a first intermediary server and transmit the one or more first requests and the token to the second document store, generate the one or more first responses, each comprising the token, corresponding to the respective one or more first requests, transmit the one or more first

responses to the first intermediary server, via a messaging bus, hash the one or more first requests and the one or more first responses to generate one or more first request hashes and one or more first response hashes, respectively and add the one or more first request hashes and the one or more first response hashes to the enriched data record in the blockchain.

[060] In one embodiment of the invention, the second intermediary server is further configured to encrypt each one of the one or more first responses with a first public key and sign the each one of the one or more first responses with a second public key, before transmission to the first intermediary server and decrypt each one of the one or more first requests with a second private key after reception from the first intermediary server.

[061] According to a seventh aspect of the invention, there is provided a second intermediary server for facilitating processing of a financial transaction, operably connected to a network and a second document store, and configured to transmit one or more second requests, each comprising a token, to a first intermediary server, via a messaging bus and receive one or more second responses from the first intermediary server and transmit the one or more second responses to the second document store.

[062] In one embodiment of the invention, the second intermediary server is further configured to hash the one or more second responses to regenerate one or more second response hashes and verify the one or more second response hashes with the blockchain, using the token.

[063] In one embodiment of the invention, the second intermediary server is further configured to encrypt each one of the one or more second requests with a first public key and sign each one of the one or more second requests with a second public key, before transmission to the first intermediary server

JPMC Ex. 1002
Page 64

and decrypt each one of the one or more second responses with a second private key after reception from the first intermediary server.

[064] In one embodiment of the invention, the second intermediary server is further configured to add the second public key into the blockchain.

[065] In one embodiment of the invention, the one or more second responses comprise one or more first regulatory compliance documents pertaining to a first user.

[066] Other aspects of the invention are also disclosed.

Brief Description of the Drawings

[067] Notwithstanding any other forms which may fall within the scope of the present invention, a preferred embodiment / preferred embodiments of the invention will now be described, by way of example only, with reference to the accompanying drawings in which:

[068] Fig. 1 illustrates a top level diagram of a system of computing devices to which various embodiments described herein may be implemented;

[069] Fig. 2 illustrates a subsystem of the computing devices for generation of a token, in accordance with a preferred embodiment of the present invention;

[070] Fig. 3 illustrates a subsystem of the computing devices for exchange of requests and responses between two intermediary servers, via a messaging bus, in accordance with a preferred embodiment of the present invention;

[071] Fig. 4 illustrates a subsystem of the computing devices for making a payment to a second user, by a first user, in accordance with a preferred embodiment of the present invention;

[072] Fig. 5 illustrates a subsystem of the computing devices for making a payment to the first user, by the second user, in accordance with a preferred embodiment of the present invention;

[073] Fig. 6 illustrates a computing device to which various embodiments described herein may be implemented; and

[074] Fig. 7 illustrates a computer implemented method for processing a financial transaction, in accordance with a preferred embodiment of the present invention;

[075] Figure 8A is a block diagram of the entities and intermediaries involved in a prior art electronic settlement system;

[076] Figure 8B is a data and funds flow according to a prior art settlement system;

[077] Figure 9A, 9B is a data and funds flow diagram according to an indicative embodiment of the present invention;

[078] Figure 9C is a block diagram of the basic infrastructure and components suited for use with embodiments of the present invention;

[079] Figure 10 A, B, C comprise block diagrams of the steps in a settlement transaction in accordance with a first preferred embodiment of the present invention;

[080] Figure 11 is a block diagram of salient characteristics of a messaging system 810 of the prior art as compared with the salient messaging characteristics of the system 1010 enabled by the code of a second embodiment;

[081] Figure 12 illustrates the options for data content to be included in tokens in accordance with embodiments of the invention as described above;

[082] Figure 13 provides a comparison of characteristics of embodiments of the present invention as compared with the prior art Swift-based messaging system;

[083] Figure 14 is a block diagram in accordance with a further preferred embodiment of the present invention;

[084] Figures 15A and15B are block diagrams of an implementation of a blockchain arrangement suitable for use with the system of embodiments of the invention;

[085] Figure 16 is a block diagram in accordance with yet a further preferred embodiment of the present invention and;

[086] Figure 17 is a detailed block diagram of the system of figure 10C and figure 16;

Description of Embodiments

[087] It should be noted in the following description that like or the same reference numerals in different embodiments denote the same or similar features.

System 100 of computing devices

[088] Fig. 1 shows a system 100 of computing devices adapted for implementation of various embodiments of the present invention.

[089] As such, the system 100 comprises a first digital device 110 and a second digital device 114 connected to a network 116. According to various embodiments, the first digital device 110 is one of, but not limited to, a mobile phone, a desktop computer, a laptop or a tablet etc. Similarly, according to various embodiments, the second digital device is one of, but not limited to, a mobile phone, a desktop computer, a laptop or a tablet etc. Further, the network 116 is one of, but not limited to, a Wide Area Network (WAN) or a Local Area Network (LAN). Preferably the network 116 is internet. The first digital device 110 and the second digital device 114 are also able to communicate through a second network 112. In one embodiment of the invention, the second network 112 is a telecommunication network such as internet or a mobile telecommunication network. In another embodiment, the second network 112 is a non-telecommunication network such as Bluetooth and Near Field Communication (NFC) etc.

[090] Further, the system 100 comprises a first intermediary server 126 and a second intermediary server 128 connected to the network 116. In one embodiment of the invention, the first intermediary server 126 and the second intermediary server 128 represent a first financial institution and a second financial institution, respectively. In one embodiment of the invention, the respective first and second financial institutions are different branches of different of different banks. In another embodiment, the respective first and second financial institutions are different branches of a single bank. In various other embodiments, the respective first and second financial institutions are, but not limited to, commercial banks, investment banks, brokerages, investment companies etc. It is to be noted that each

one of the first intermediary server 126 and the second intermediary server 128 may represent a system of servers comprising web servers, application servers, database servers and gateway servers.

[091] Further, the first intermediary server 126 is operably connected to a first document store 132 and the second intermediary server 128 is operably connected to the second document store 134. In one embodiment, the first document store 132 and the second document store 134 represent databases configured to store a plurality of documents. Each one of the documents comprise data pertaining to a financial transaction and metadata corresponding to the data. In various embodiments, metadata comprises format, encoding, author, hash, verification and relationships to other documents.

[092] Further, the system 100 comprises a financial messaging server 130 connected to the network 116. The financial messaging server 130 provides a financial messaging service between any two intermediary servers, including the first intermediary server 126 and the second intermediary server 128. Some of the examples of financial messaging services include SWIFT (Society for Worldwide Interbank Financial Telecommunication) for cross border transactions. ACH (Automated Clearing House) used in USA and RTGS (Real Time Gross Settlement) used in India and Hong Kong.

[093] Further, the system 100 comprises a token server 120 connected to the network 116 and a token database 122. Further, a blockchain 124 is connected to the network 116. Further, a messaging bus 118 is connected to the network 116. The messaging bus 118 represents a messaging server or a system of messaging servers configured to enable a plurality of applications/servers/devices to communicate with each other. In one embodiment, the messaging bus 118 also comprises an authentication/ authorization server for authorizing the computing devices communicating

through the messaging bus 118. The detailed configuration of the messaging bus 118 has been described in the discussion to follow.

[094] Also, a blockchain 124 is connected to the network 116. The configuration and/or the functioning of the first intermediary server 126, the second intermediary server 128, the first document store 132, the second document store 134, the token server 120, the token database 122, the blockchain 124, and the messaging bus 118 has been described below in a description. The system 100 for processing a financial transaction involves subsystems of the computing devices, which have been depicted by means of figures and description as following. The description below has been explained with embodiments comprising a financial transaction between a first user and a second user. In some embodiments, the first user acts as a biller/ beneficiary/payee and the second user acts as purchaser/payer. In other embodiments, the first user acts as a payer and the second user acts as a payee/beneficiary. Further, it is to be noted that the first user and the second user may represent any number of entities involved in the financial transaction.

[095] In one embodiment of the invention, the first user may instruct the first intermediary sever 126 to process the financial transaction. In one embodiment, the financial transaction involves generation of an invoice for the second user and receiving a payment from the second user, by the first user. In another embodiment, the financial transaction involves making the payment to the second user, by the first user. Specifically, the first user connects with the first intermediary server 126 through the network 116, using the first digital device 110.

[096] Figure 2 illustrates a subsystem (200) of the computing devices for generation of a token, in accordance with a preferred embodiment of the present invention. As shown in figure 2, the first digital device 110

comprises a first processor 210 operably connected to a first memory 220. The first memory 220 comprises a first computer program code, the first computer program code when executed by the first processor 210 instructs the first processor 210 to instruct the first intermediary server 126 to process the financial transaction. Further, in one embodiment of the invention, the first computer program code further instructs the first processor 210 to provide one or more documents pertaining to the financial transaction, to the first intermediary server 126. In another embodiment, the one or more documents are already available with the first intermediary server 126. In yet another embodiment, the first intermediary server 126 is configured to generate at least one document from the one or more documents.

[097] The at least one document may be, but is not limited to, a request for processing the financial transaction. The first intermediary server 126 is configured to transmit the one or more documents pertaining to the financial transaction, to the first document store 132. In one embodiment of the invention, the one or more documents comprise payment metadata such as, but is not limited to, account numbers of the first user (or a beneficiary), Business Identifier Codes (BIC) of the financial institutions corresponding to the first intermediary server 126 and the second intermediary server 128, amount of currency to be transferred and type of currency etc.

[098] Further, in accordance with an embodiment, the one or more documents comprise one or more first regulatory compliance documents pertaining to the first user. Some examples of the regulatory compliance documents include, but are not limited to purpose of payment documents, a result of sanctions screening and secondary identifiers such as date of birth proof, address proof or other Know Your Customer (KYC) documents.

[099] The first intermediary server 126 is further configured to generate an enriched data record from the one or more documents and add the enriched

data record into the blockchain 124. The first intermediary server 126 is configured to generate the enriched data record in multiple ways in multiple embodiments, some of the embodiments have been elucidated below.

[0100] In one embodiment of the invention, the first intermediary server 126 is configured to extract a plurality of attributes from the one or more documents. The plurality of attributes may comprise, but are not limited to, originator attributes, beneficiary attributes and purpose of payment etc. Further, the first intermediary server 126 is configured to combine the plurality of attributes to generate the enriched data record. In another embodiment of the present invention, the first intermediary server 126 is configured to extract the plurality of attributes from one or more documents, de-identify the plurality of attributes to obtain a plurality of de-identified attributes and combine the plurality of de-identified attributes to generate the enriched data record. In yet another embodiment of the present invention, the first intermediary server 126 is configured to extract the plurality of attributes from the one or more documents, hash the plurality of attributes to generate a plurality of respective hashes and combine the plurality of hashes to generate the enriched data record.

[0101] Further, the blockchain 124 is a data structure comprising a plurality of blocks of data. Each block of data from the plurality of blocks of data represents a single financial transaction. Further, the blockchain 124 is configured to store data pertaining to the financial transaction in association with the token. The data pertaining to the financial transaction includes, but is not limited to, the enriched data record, a plurality of hashes, a plurality of public keys etc. Also the blockchain 124 is configured to return the data pertaining to the financial transaction, when queried using the token.

[0102] Further, the first intermediary server 126 is configured to request generation of a token, to the token server 120, via the messaging bus 118.

The token server 120 in turn is configured to generate the token and add the token into the blockchain 124. The token is stored in the blockchain 124, in association with the enriched data record. Further, the token server 120 is configured to transmit the token to the first intermediary server 126, via the messaging bus 118. Further, the first intermediary server 126 is configured to transmit the token to the first document store 132. The token is stored in the first document store 132, in association with the one or more documents.

[0103] In one embodiment of the invention, the token server 120 is further configured to implement a smart contract and add the smart contract into the blockchain 124. In one embodiment, the smart contract is a shared, signed and verifiable program code which is distributed and/or executed on the blockchain 124. The smart contract would run on the blockchain 124 and would be stored in association with the token.

[0104] In one embodiment of the invention, before proceeding any further, the first intermediary server 126 may wish to perform certain "checks", by communicating with the second intermediary server 128, via the messaging bus 118. For enabling communication, the first intermediary server 126 is configured to generate a first asymmetrical pair of a first public key and a first private key. Further, the first intermediary server 126 is configured to add the first public key and a first address of the first intermediary server 126 into the blockchain 124. Similarly, the second intermediary server 128 is configured to generate a second asymmetrical pair of a second public key and a second private key. Further, the second intermediary server 128 is configured to add the second public key and a second address of the second intermediary server 128 into the blockchain 124.

[0105] Fig. 3 illustrates a subsystem (300) of the computing devices for exchange of requests and responses between the first intermediary server

126 and the second intermediary server 128, via the messaging bus118, in accordance with a preferred embodiment of the present invention. During communication with the second intermediary server 128, the first intermediary server 126 is configured to transmit one or more first requests, each comprising the token, to the second intermediary server 128, via the messaging bus 118. Examples of one or more first requests comprise, but are not limited to, KYC check and payment acceptance. In one embodiment of the invention, the the one or more first requests are transmitted on basis of a plurality of predefined criterion. For example, if the first intermediary server 126 is required to make the payment to the second intermediary server 128, the first intermediary server 126 may necessitate KYC check of the second user. The second intermediary server 128 is configured to then receive the one or more first requests from the first intermediary server 126 and transmit the one or more first requests and the token to the second document store 134. In one embodiment of the invention, the one or more first requests are transmitted to the second documents store 134 in form of one or more first request documents.

[0106] Further, the second intermediary server 128 is configured to generate one or more first responses, each comprising the token, corresponding to the respective one or more first requests. In one embodiment of the invention, the one or more first responses are generated in form of one or more first response documents at the second intermediary server 128. Further, the second intermediary server 128 is configured to transmit the one or more first responses to the first intermediary server 126, via the messaging bus 118. As an extension of the example above, the second intermediary server 128 may then send a validation successful response to the first intermediary server 126, via the messaging bus 118. In one embodiment of the invention, the one or more first responses comprise one or more second regulatory compliance documents pertaining to a second user.

JPMC Ex. 1002
Page 74

[0107] Further, the second intermediary server 128 is configured to hash the one or more first requests and the one or more first responses to generate one or more first request hashes and one or more first response hashes, respectively. Also, the second intermediary server 128 is configured to add the one or more first request hashes and the one or more first response hashes to the enriched data record in the blockchain 124. The first intermediary server 126 is then configured to receive the one or more first responses and transmit the one or more first responses to the first document store 132. In one embodiment of the invention, the first intermediary server 126 is further configured to hash the one or more first responses to regenerate the one or more first response hashes. Further, the first intermediary server 126 is configured to verify the one or more first response hashes with the blockchain 124, using the token. The first intermediary server 126 can ensure that the one or more first responses are same as the ones generated at the second intermediary server 128.

[0108] In one embodiment of the invention, to enable secure transmission, the first intermediary server 126 is configured to encrypt each one of the one or more first requests with the second public key and sign each one of the one or more first requests with the first public key, before transmission to the second intermediary server 128. Consequently, the second intermediary server 128 is configured to decrypt the each one of the one or more first requests with the second private key after reception from the first intermediary server 126. In a similar manner, the second intermediary server 128 is configured to encrypt each one of the one or more first responses with the first public key and sign the each one of the one or more first responses with the second public key, before transmission to the first intermediary server 126. Consequently, the first intermediary server 126 is configured to decrypt each one of the one or more first responses with the first private key after reception from the second intermediary server 128.

[0109] The second intermediary server 128 may also request certain compliance checks. Therefore, the second intermediary server 128 is further configured to transmit one or more second requests, each comprising the token, to the first intermediary server 126, via the messaging bus 118. Examples of the one or more second requests comprise, but are not limited to, sender sanctions screening check. The first intermediary server 126 is in turn configured to receive the one or more second requests and transmit the one or more second requests to the first document store 132. In one embodiment of the invention, the one or more second requests are transmitted to the first document store 132 in form of one or more second request documents. Further the first intermediary server 126 is configured to generate one or more second responses, each comprising the token, corresponding to the respective one or more second requests. In one embodiment of the invention, the one or more second responses are generated in form of one or more second response documents. Further, the first intermediary server 126 is configured to transmit the one or more second responses to the second intermediary server 128, via the messaging bus 118. In one embodiment of the invention, the one or more second responses comprise the one or more first regulatory compliance documents pertaining to the first user.

[0110] Further, the first intermediary server 126 is configured to hash the one or more second requests and the one or more second responses to generate one or more second request hashes and one or more second response hashes, respectively. Further, the first intermediary server 126 is configured to add the one or more second request hashes and the one or more second response hashes to the enriched data record in the blockchain 124. The second intermediary server 128 is in turn configured to receive the one or more second responses and transmit the one or more second responses to the second document store 134. In one embodiment of the

invention, the second intermediary server 128 is further configured to hash the one or more second responses to regenerate the one or more second response hashes and verify the one or more second response hashes with the blockchain 124, using the token. Thus ensuring that the one or more second responses are same as those generated at the first intermediary server 126.

[0111] In one embodiment of the invention, to enable secure communication, the second intermediary server 128 is configured to encrypt each one of the one or more second requests with the first public key and sign each one of the one or more second requests with the second public key, before transmission to the first intermediary server 126. Consequently, the first intermediary server 126 is configured to decrypt the each one of the one or more second requests with the first private key after reception from the second intermediary server 128. In a similar manner, the first intermediary server 126 is configured to encrypt each one of the one or more second responses with the second public key and sign the each one of the one or more second responses with the first public key, before transmission to the second intermediary server 128. Consequently, the second intermediary server 128 is configured to decrypt the each one of the one or more second responses with the second private key after reception from the first intermediary server 126.

[0112] The requests and the responses are transmitted in a secure manner across the messaging bus 118, in form of a plurality of messages. It is to be noted that each one of the plurality of messages comprises a content hash of all its contents to ensure that the contents have not been altered during transmission. The request and/or receipt time of the recipient public key are also attached to the plurality of messages. This ensures only recipient can see message contents & ensures revocability of public keys.

[0113] In one embodiment of the invention, the first intermediary server 128 is further configured to assign a payment risk rating to the token. In one embodiment of the invention, the payment risk rating is assigned to the token at the first intermediary server 126 after completion of the communication with the second intermediary server 128. The payment risk rating provides a pointer to the regulatory and other compliance checks performed by the first intermediary server 126 and the second intermediary server 128. In one embodiment of the invention, the first intermediary server 126 is further configured to add the payment risk rating to the enriched data record in the blockchain 124. Further, the blockchain 124 is configured to return the payment risk rating when queried with the token. The payment risk rating enables better straight through processing by reducing exceptions and false positives.

[0114] The token thus generated may be used to make the payment to the second user by the first user or making the payment to the first user, by the second user. Figure 4 illustrates a subsystem (400) of the computing devices for making the payment to the second user, by the first user. As shown in the figure 4, the first intermediary server 126 is configured to send a first financial message comprising the token, to the second intermediary server 128, indicative of making the payment to the second user. The first financial message is sent through the financial messaging server 130.

[0115] Figure 5 illustrates a subsystem (500) of computing devices for making the payment to the first user, by the second user. As shown in the figure 5, the first intermediary server 126 is further configured to transmit the token to the first digital device 110. In turn, the first computer program code instructs the first processor 210 to receive the token from the first intermediary server 126. In one embodiment of the invention, the first processor 210 is further instructed to provide the token to the second digital device 114 via the network 116 or the second network 112. The second

digital device 110 comprises a second memory 520 and a second processor 510 operably connected to the second memory 520, the second memory 520 comprising a second computer program code, the second computer program code when executed by the second processor 510, instructs the second processor 510 to receive the token from the first digital device 110 and provide the token to the second intermediary server 128.

[0116] In turn the second intermediary server 128 is configured to receive the token from the second digital device 114, transmit the token to the second document store 134 and send a second financial message comprising the token, to the first intermediary server 126, indicative of making the payment to the first user. Further, the second financial message is sent through the financial messaging server 130.

Computing device

[0117] Fig. 56 shows a computing device 600. In a preferred embodiment, the computing device 600 takes the form of the first intermediary server 126, the second intermediary server 128, the token server 120 and the financial messaging server 190 as described above. In this manner, the computing device 500 is adapted to comprise functionality for communication with the network 116, storage capability (such as the token database 122) for storing a plurality of tokens and respective creators of the plurality of tokens.

[0118] However, it should be noted that each one first digital device 110 and the second digital device 114, as shown in figure 1, may also be depicted as the computing device 600. In this manner, the computing device may comprise differing technical integers, such as the display device 6020, one or more human interface devices 660 and the like. In other words, the technical integers of the computing device 500 is shown in figure 5 are exemplary only and variations, adaptations and the like may be made

thereto within the purposive scope of the embodiments described herein and having regard for the particular application of the computing device 600.

[0119] In particular the steps of the computer implemented method for processing of a financial transaction, as described in further detail below, may be implemented as computer program code instructions executable by the computing device 600. The computer program code instructions may be divided into one or more computer program code instruction libraries, such as dynamic link libraries (DLL), wherein each of the libraries performs a one or more steps of the computer implemented method. Additionally, a subset of the one or more of the libraries may perform graphical user interface tasks relating to the steps of the computer implemented method.

[0120] The device 600 comprises semiconductor memory 610 comprising volatile memory such as random access memory (RAM) or read only memory (ROM). The memory 600 may comprise either RAM or ROM or a combination of RAM and ROM.

[0121] The device 600 comprises a computer program code storage medium reader 630 for reading the computer program code instructions from computer program code storage media 620. The storage media 620 may be optical media such as CD-ROM disks, magnetic media such as floppy disks and tape cassettes or flash media such as USB memory sticks.

[0122] The device further comprises I/O interface 640 for communicating with one or more peripheral devices. The I/O interface 640 may offer both serial and parallel interface connectivity. For example, the I/O interface 640 may comprise a Small Computer System Interface (SCSI), Universal Serial Bus (USB) or similar I/O interface for interfacing with the storage medium reader 630. The I/O interface 640 may also communicate with the one or more human interface devices (HID) 660 such as keyboards, pointing devices,

joysticks and the like. The I/O interface 640 may also comprise a computer to computer interface, such as a Recommended Standard 232 (RS-232) interface, for interfacing the device 600 with one or more personal computer (PC) devices 690. The I/O interface 640 may also comprise an audio interface for communicate audio signals to one or more audio devices 6050, such as a speaker or a buzzer.

[0123] The device 600 also comprises a network interface 650 for communicating with one or more computer networks 680. The network 680 may be a wired network, such as a wired Ethernet™ network or a wireless network, such as a Bluetooth™ network or IEEE 802.11 network. The network 680 may be a local area network (LAN), such as a home or office computer network, or a wide area network (WAN), such as the Internet or private WAN.

[0124] The device 600 comprises an arithmetic logic unit or processor 6000 for performing the computer program code instructions. The processor 6000 may be a reduced instruction set computer (RISC) or complex instruction set computer (CISC) processor or the like. The device 600 further comprises a storage device 6030, such as a magnetic disk hard drive or a solid state disk drive.

[0125] Computer program code instructions may be loaded into the storage device 6030 from the storage media 620 using the storage medium reader 630 or from the network 680 using network interface 650. During the bootstrap phase, an operating system and one or more software applications are loaded from the storage device 6030 into the memory 610. During the fetch-decode-execute cycle, the processor 6000 fetches computer program code instructions from memory 610, decodes the instructions into machine code, executes the instructions and stores one or more intermediate results in memory 600.

JPMC Ex. 1002
Page 81

[0126] In this manner, the instructions stored in the memory 610, when retrieved and executed by the processor 6000, may configure the computing device 600 as a special-purpose machine that may perform the functions described herein.

[0127] The device 600 also comprises a video interface 6010 for conveying video signals to a display device 6020, such as a liquid crystal display (LCD), cathode-ray tube (CRT) or similar display device.

[0128] The device 600 also comprises a communication bus subsystem 665 for interconnecting the various devices described above. The bus subsystem 665 may offer parallel connectivity such as Industry Standard Architecture (ISA), conventional Peripheral Component Interconnect (PCI) and the like or serial connectivity such as PCI Express (PCIe), Serial Advanced Technology Attachment (Serial ATA) and the like.

Embodiments of the method

[0129] Figure 7 illustrates a computer implemented method 700 for processing a financial transaction in accordance with an embodiment of the present invention. As described above, the financial transaction is assumed to be taking place between the first user and the second user. The method begins at step 710 by transmitting the one or more documents pertaining to the financial transaction, from the first intermediary server 126 to the first document store 132. In one embodiment of the invention, the one or more documents are provided to the first intermediary server 126 by the first user, from the first digital device 110. In another embodiment, the one or more documents are already available with the first intermediary server 126. In yet another embodiment, the at least one document from the one or more documents is generated at the first intermediary server 126.

[0130] At step 720, the enriched data record is generated from the one or more documents, at the first intermediary server 126. Further, the enriched data record is added into the blockchain 124, from the first intermediary server 126. The enriched data record may be generated in different manners in different embodiments. Some of the embodiments have been discussed below.

[0131] In one embodiment of the invention, the plurality of attributes are extracted from the one or more documents, at the first intermediary server 126. Further, the plurality of attributes are combined to generate the enriched data record at the first intermediary server 126.

[0132] In another embodiment, the plurality of attributes are extracted from the one or more documents, at the first intermediary server 126. Further, the plurality of attributes are de-identified to obtain the plurality of de-identified attributes at the first intermediary server 126. The de-identification of the plurality of attributes comprises removal of any information from the plurality of attributes which may link the plurality of attributes to the first user or the second user. This is to ensure the confidentiality of the first user and the second user, in case the enriched data record is accessed through illegal routes. The plurality of de-identified attributes are then combined, at the first intermediary server 126, to generate the enriched data record.

[0133] In yet another embodiment, the plurality of attributes are extracted from the one or more documents, at the first intermediary server 126. Further, the plurality of attributes are hashed to generate the plurality of respective hashes, at the first intermediary server 126. The plurality of hashes are then combined to generate the enriched data record, at the first intermediary server 126.

[0134] At step 730, the token server 120 is requested to generate the token corresponding to the financial transaction, from the first intermediary server 126, via the messaging bus 118. At step 740, the token is generated at the token server 120. Further, the token is added into the blockchain 124, from the token server 120. At step 750, the token is transmitted from the token server 120 to the first intermediary server 126. At step 760, the token is transmitted from the first intermediary server 126 to the first document store 132. Further, the token is stored in association with the one or more documents, in the first document store 132.

[0135] In one embodiment of the invention, the smart contract is implemented at the token server 120. Further, the smart contract is added into the blockchain, from the token server 120.

[0136] In one embodiment of the invention, the first intermediary server 126 communicates with the second intermediary server 128, via the messaging bus 118. The communication may take place for verification and validation of the first user and the second user. In one embodiment of the invention, the first asymmetrical pair of the first public key and the first private key is generated at the first intermediary server 126. Further, the first public key and the first address of the first intermediary server 126 are added into the blockchain 124, from the first intermediary server 126. Similarly, the second asymmetrical pair of the second public key and the second private key is generated at the second intermediary server. Further, the second public key and the second address of the second intermediary server 128 are added into the blockchain 124, from the second intermediary server 128.

[0137] In one embodiment, during communication, the one or more first requests, each comprising the token, are transmitted from the first intermediary server 126 to the second intermediary server 128, via the messaging bus 118. Further, the one or more first requests are received at

the second intermediary server 128 and the one or more first requests and the token are transmitted from the second intermediary server 128 to a second document store 134. Further, one or more first responses, each comprising the token, corresponding to the respective one or more first requests, are generated at the second intermediary server 128. Further, the one or more first responses are transmitted from the second intermediary server 128 to the first intermediary server 126, via the messaging bus 118. Further, the one or more first requests and the one or more first responses are hashed at the second intermediary server 128 to generate one or more first request hashes and one or more first response hashes, respectively. Further, the one or more first request hashes and the one or more first response hashes are added to the enriched data record in the blockchain 124, from the second intermediary server 128. Also, the one or more first responses are received at the first intermediary server 126 and transmitted to the first document store 132.

[0138] In one embodiment of the invention, the one or more first responses comprise the one or more second regulatory compliance documents pertaining to the second user. Further, in one embodiment of the invention, the one or more first responses are hashed at the first intermediary server 126 to regenerate the one or more first response hashes. Also, the one or more first response hashes are verified with the blockchain 124 from the first intermediary server 126, using the token.

[0139] In one embodiment of the invention, for secure communication, each one of the one or more first requests are encrypted with the second public key and signed with the first public key at the first intermediary server 126, before transmission to the second intermediary server 128. Consequently, the each one of the one or more first requests are decrypted with the second private key at the second intermediary server 128 after reception from the first intermediary server 126. Similarly, each one of the one or more first

responses are encrypted with the first public key and signed with the second public key at the second intermediary server 128, before transmission to the first intermediary server 126. Also, consequently, the each one of the one or more first responses are decrypted with the first private key at the first intermediary server 126 after reception from the second intermediary server 128.

[0140] Similarly, in the present and various other embodiments, during communication, the one or more second requests, each comprising the token, are transmitted from the second intermediary server 128 to the first intermediary server 126, via the messaging bus 118. Further, the one or more second requests are received at the first intermediary server 126 and the one or more second requests are transmitted from the first intermediary server 126 to the first document store 132. Further, one or more second responses, each comprising the token, corresponding to the respective one or more second requests, are generated at the first intermediary server 126. Further, the one or more second responses are transmitted from the first intermediary server 126 to the second intermediary server 128, via the messaging bus 118. Further, the one or more second requests and the one or more second responses are hashed at the first intermediary server 126 to generate one or more second request hashes and one or more second response hashes, respectively. Further, the one or more second request hashes and the one or more second response hashes are added to the enriched data record in the blockchain 124, from the first intermediary server 126. Also, the one or more second responses are received at the second intermediary server 128 and transmitted to the second document store 134.

[0141] In one embodiment of the invention, the one or more second responses comprise the one or more first regulatory compliance documents pertaining to the first user. Further, in one embodiment, the one or more second

responses are hashed at the second intermediary server 128 to regenerate the one or more second response hashes. Also, the one or more second response hashes are verified with the blockchain 124 from the second intermediary server 128, using the token.

[0142] In one embodiment of the invention, for secure communication, each one of the one or more second requests are encrypted with the first public key and signed with the second public key at the second intermediary server 128, before transmission to the first intermediary server 126. Consequently, the each one of the one or more second requests are decrypted with the first private key at the first intermediary server 126 after reception from the second intermediary server 128. Similarly, each one of the one or more second responses are encrypted with the second public key and signed with the first public key at the first intermediary server 126, before transmission to the second intermediary server 128, and decrypted with the second private key at the second intermediary server 128 after reception from the first intermediary server 126.

[0143] In one embodiment of the invention, the payment risk rating is assigned to the token, at the first intermediary server 126. Further, the payment risk rating is added to the enriched data record in the blockchain 124, from the first intermediary server 126.

[0144] In one embodiment, for making the payment to second user, by the first user, the first financial message comprising the token, is sent from the first intermediary server 126 to the second intermediary server 128, indicative of making the payment to the second user. Further, the first financial message is sent via the financial messaging server 130.

[0145] In another embodiment, the token is transmitted from the first intermediary server 126 to the first digital device 110, available with the first

user. The first processor 210 receives the token from the first intermediary server 126 and stores the token in the first memory 220. Further, the token is provided to the second user, by the first user. In one embodiment, the token is provided to the second user by means of a Quick Response (QR) code printed on an invoice. In another embodiment, the token is provided to the second user at the second digital device 114 available with the second user, from the first digital device 110. The second processor 510 receives the token from the first digital device 110, and stores the token in the second memory 520.

[0146] Further, the token is provided to the second intermediary server 128, from the second digital device 114, by the second user. The second computer program code instructs the second processor 510 to provide the token to the second intermediary server. The token is then transmitted to the second document store 134, from the second intermediary server 128. Further, the second financial message is sent from the second intermediary server 128, to the first intermediary server 126, indicative of making the payment to the first user.

Prior Art

[0147] With reference to Figure 8A there is illustrated in block form the basic components of a prior art settlement system. In many transactions there will be an at least first transacting entity 811 which enters into a financial transaction with an at least second transacting entity 812. The financial transaction may be as simple as the agreement by the first transacting entity 811 to sell a particular item or service to the second transacting entity 812. Typically the financial transaction will require settlement for an agreed amount expressed in a Fiat or other currency. In the vast majority of cases the at least first transacting entity 811 will be associated with an at least first

intermediary entity 813, in this instance in the form of a bank A and similarly the second transacting entity 812 will be associated with an at least second intermediary entity 814 in this instance in the form of bank B. The first transacting entity 811 will have a first bank account 815 at the first intermediary entity 813 whilst second transacting entity 812 will have a second bank account 816 at second intermediary entity 814. Settlement of any given transaction requires instruction given by first transacting entity 811 to its first intermediary entity 813 to pay an agreed amount from the first bank account 815 to the bank account comprising second bank account 816 of second intermediary entity 814 of second transacting entity 812. For these instructions to be carried out metadata in the form of payment metadata 817 must be assembled at the first intermediary entity 813 sufficient and exhaustive to communicate to the second intermediary entity 814 such that the agreed settlement amount is transmitted from bank A to bank B and more particularly to the specific accounts of the respective first transacting entity 811 and second transacting entity 812.

[0148] A similar transaction may be applied in reverse where the second transacting entity sells a good or service to first transacting entity 811. In such an instance the respective intermediaries, once having received the respective payment metadata 817 and exchanged that metadata 817 may elect to simply pay the difference 818 electronically as between the intermediaries to effect the multiple transactions. In some instances, particularly where the financial transaction is cross-border-for example the first intermediary entity 813 is in a first country whilst the second intermediary entity 814 is in a second country the metadata 817 may include what is known as a Swift code which is a substantially unique identifier for each intermediary entity involved in the financial transaction. However, for any given transaction, far more data than merely a unique identifier for each intermediary entity involved in a financial transaction is required in order for

the appropriate settlement amounts to ultimately be recorded in the correct accounts and settle the financial transaction for the agreed amounts.

[0149] Figure 8B is a data and funds flow diagram of data and funds flow according to a prior art settlement system at the granular level. In this instance, with reference to figure 8B like components are numbered as for figure 8A a given transaction requiring settlement can be embodied as a bill 890 which will include payment data 891 and may include bank facilitation payment data 892 comprising, in this instance, a biller code and a financial transaction code. Banks which are party to this bank facilitation payment system permit data entry by entity B (or payer B) 812 into a database of bank B 814 by means of a bank application or web interface 814 B. Bank B may then add additional data to form metadata 817 which is sent to a third-party server 893 which utilises metadata 817 to trigger pay (settlement) of bill 890 from payer B bank 814 to biller A bank 813.

Exemplary Embodiments

[0150] With reference to Figure 9C there is illustrated a block diagram of the basic infrastructure and components suited for use with embodiments of the present invention. In this instance like components are numbered as for figure 8 except in the 900 series. So, for example, first transacting entity 811 becomes first transacting entity 911 in this embodiment with reference to figure 2C.

[0151] In this instance a settlement system 910 according to a generalised embodiment includes at least first transacting entity 911 which enters into a financial transaction with at least a second transacting entity 912. As previously these entities are associated with a respective first intermediary entity 913 and a second intermediary entity 914 in the form of bank A and

bank B. Each of the first transacting entity 911 and a second transacting entity 912 has a respective account 915, 916 at their respective intermediary entities as illustrated in figure 9C

[0152] In this instance, in the event that first transacting entity 911 enters into a financial transaction with second transacting entity 912 then, at the time of entry into the financial transaction 920, a token 921 is generated. In this instance the token 921 is generated by at least first digital device 922 communicating with a token database 923. The token database 923 generates a token comprising a data file 924 containing all data that will ultimately be required to settle the financial transaction 920 including any necessary identifying information for the transacting entity is, their accounts and the intermediary entities. Settlement is effected by communication of the token 921 to bank A and then to bank B together with the appropriate flow of funds.

[0153] With reference to figure 9A at the granular level a bill 990 from a biller 911 directed to a payer 912 contains bill data 991 and also token data of a token 921 residing within a code symbol 994 (in this instance a QR code). The token data includes pointer data pointing to data 995 on token database 923. The data 995 combined with bank ID data 914 permits the creation by token database 923 of a full payment record 996 which can be utilised to cause settlement of the bill 990 as against payer 912 via, in this instance, their respective banks 914, 913.

[0154] With reference to figure 9B the payment data record 996 is utilised has fed into a settlement network such as, for example a network 997 operating under the Ripple protocol thereby permitting substantially real-time settlement across multiple institutions and banks.

[0155] With reference to Figures 10 there is illustrated in block diagram form a first preferred embodiment of the present invention by way of a non-limiting example of a financial transaction. In this embodiment like components are numbered as for the previous embodiments except in the 1000 series. So, for example, token 921 becomes token 1021.

[0156] With reference to figure 10A the financial transaction system 1010 is activated, as for the previous embodiment, when a financial transaction 1020 is entered into between at least first transacting entity 1011 and at least a second transacting entity 1012 each dealing, for the purposes of this transaction, through respective intermediary entities 1013, 1014.

[0157] At the time of and as part of entry into the financial transaction 1020 the first transacting entity 1011 accesses token database 1023 via digital device 1022 executing via a web browser interface or via execution of an application running on a portable digital devices such as a mobile telephone or in a further alternative as a point-of-sale terminal in order to arrange for the database 1023 to generate a token 1021. In this instance the token 1021 will include better data 1024 including the recipient named, BIC, IBAN, destination country, mobile number, currency, business type, communication, payment amount. In this instance the token 1021 including the metadata 1024 is stored in the token database 1023. In addition the first transacting entity 1011 communicates the token 1021 to a digital device 1030 associated with second transacting entity 1012. In this instance the communication is by way of initial transmission of the token 1021 to digital device 1022 which then on transmits the token via Internet 1031 to digital device 1030.

[0158] With reference to figure 10B, when ready to settle the financial transaction 1020 the second transacting entity 1012 "logs in" to a portal associated with second intermediary entity 1014 and communicates the

token 1021. In this instance have the login can be executed via a web browser associated with digital device 1030 which communicates via Internet 1031 the token 1021 to a digital processing system 1032 (including at least a processor and a memory) associated with second intermediary entity 1014. Substantially at the same time as part of seeking to settle the financial transaction 1020:

[0159] Notification: token database 1023 notifies second intermediary entity 1014 to contact the token database 1023 from which it receives a further token 1021A.

[0160] Verification: token database 1023 communicates with the processing system 1032 of second intermediary entity 1014 to verify that sufficient funds are located in account 1016 as indicated in the meta data 1024 to settle the financial transaction.

[0161] Committing payer funds: payers bank debits payers account: payers bank sends notice to payer bank gateway: payers bank gateway calls token database 1023 to get approved token:

[0162] Settlement: gateway of payers bank sends by way of non-limiting example XRP (the native currency of the Ripple protocol) to billers bank gateway: payers bank gateway notifies token database 1023 of receipt:

[0163] Clearing: payer's bank Nostro account is debited subject to bank institution rules.

[0164] Examples of tokenised messages and their generation and transmission are illustrated in pseudocode ~~below~~at the end of the description before the claims. Reference to "sparro" is a reference to an instance of a token databasep23.

[0165] The previous, meta-data mode is first. It switches to minimal half way through

---

[0166] Bank:HSBC >> createUserCode >> Sparro:Sparro

[0166] {"id":"User:ABC Paper","name":"ABC Paper"}

[0166] (Creating Sparro User Code - Meta-data given can be used by other banks for compliance and for confirming payee with customers.)

[0166] ---

[0166] Bank:MayBank >> createUserCode >> Sparro:Sparro

[0166] {"id":"User:XYZ Printing","name":"XYZ Printing"}

[0166] (Creating Sparro User Code - Meta-data given can be used by other banks for compliance and for confirming payee with customers.)

[0166] ---

[0166] Sparro:Sparro >> createUserCode-reply >> Bank:HSBC

[0166] {"id":"User:ABC Paper","name":"ABC Paper","code":"65q3gdd"}

[0166] ---

[0166] Sparro:Sparro >> createUserCode-reply >> Bank:MayBank

[0166] {"id":"User:XYZ Printing","name":"XYZ Printing","code":"70wqgx6"}

[0166] ---

[0166] User:ABC Paper >> createInvoice >> Bank:HSBC

[0166] {"amount":{"amount":1000,"currency":"gbp"}}

[0166] ---

[0166] Bank:HSBC >> createInvoiceCode >> Sparro:Sparro

[0166] {"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd"}

[0166] (Creating Invoice Code - An invoice code is created by Sparro and connected to the bank.)

[0166] ---

[0167] Sparro:Sparro >> createInvoiceCode-reply >> Bank:HSBC

[0167] {"code":"6tq6wcbad"}

[0167] —

[0167] Bank:HSBC >> createInvoice-reply >> User:ABC Paper

[0167] {"invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

[0167] Abc invoice { amount: { amount: 1000, currency: 'gbp' },

[0167] payee: '65q3gdd',

[0167] code: '6tq6wcbad' }

[0167] —

[0167] User:ABC Paper >> invoice >> User:XYZ Printing

[0167] {"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}

[0167] —

[0167] User:XYZ Printing >> payInvoice >> Bank:MayBank

[0167] {"invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300}}

[0167] —

[0167] Bank:MayBank >> sendMoney >> BankGateway:MayBank

[0167] {"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300}}

[0167] —

[0167] BankGateway:MayBank >> getInvoice >> Sparro:Sparro

[0167] "6tq6wcbad"

[0167] (Sending Payment to Invoice - The payment is sent to the bank that created the invoice.)

[0167] —

[0168] Sparro:Sparro >> getInvoice-reply >> BankGateway:MayBank

[0168]

{"bank":"Bank:HSBC","invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

[0168] --

[0168] BankGateway:MayBank >> transfer >> BankGateway:HSBC

[0168]

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":"ripple-1"}

[0168] --

[0168] BankGateway:HSBC >> incomingTransfer >> Bank:HSBC

[0168]

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":"ripple-1"}

[0168] --

[0168] BankGateway:HSBC >> transfer-reply >> BankGateway:MayBank

[0168] {"success":true,"owed":{"GBP":300}}

[0168] --

[0168] Bank:HSBC >> getInvoice >> Sparro:Sparro

[0168] "6tq6wcbad"

[0168] --

[0168] BankGateway:MayBank >> sendMoney-reply >> Bank:MayBank

[0168]

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":"ripple-1"}

[0168] --

[0168] Sparro:Sparro >> getInvoice-reply >> Bank:HSBC

[0169]

{"bank":"Bank:HSBC","invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

[0169] ---

[0169] Bank:MayBank >> payInvoice-reply >> User:XYZ Printing

[0169]

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":"ripple-1"}

[0169] XYZ part-paid invoice {

[0169] "payer": "70wqgx6",

[0169] "invoice": "6tq6wcbad",

[0169] "amount": {

[0169] "currency": "GBP",

[0169] "amount": 300

[0169] },

[0169] "id": "ripple-1"

[0169] }

[0169] ---

[0169] Bank:HSBC >> incomingTransfer >> User:ABC Paper

[0169]

{"invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"},"transfer":{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":"ripple-1"}}

[0169] ---

[0169] User:XYZ Printing >> payInvoice >> Bank:MayBank

[0169] {"invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700}}

[0169] ---

[0170] Bank:MayBank >> sendMoney >> BankGateway:MayBank

[0170]

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700}}

[0170] —

[0170] BankGateway:MayBank >> getInvoice >> Sparro:Sparro

[0170] "6tq6wcbad"

[0170] (Sending Payment to Invoice - The payment is sent to the bank that created the invoice.)

[0170] —

[0170] Sparro:Sparro >> getInvoice-reply >> BankGateway:MayBank

[0170]

{"bank":"Bank:HSBC","invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

[0170] —

[0170] BankGateway:MayBank >> transfer >> BankGateway:HSBC

[0170]

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700},"id":"ripple-2"}

[0170] —

[0170] BankGateway:HSBC >> incomingTransfer >> Bank:HSBC

[0170]

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700},"id":"ripple-2"}

[0170] —

[0171] BankGateway:HSBC >> transfer-reply >> BankGateway:MayBank

[0171] {"success":true,"owed":{"GBP":1000}}

[0171] --

[0171] Bank:HSBC >> getInvoice >> Sparro:Sparro

[0171] "6tq6wcbad"

[0171] --

[0171] BankGateway:MayBank >> sendMoney-reply >> Bank:MayBank

[0171]

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700},"id":"ripple-2"}

[0171] --

[0171] Sparro:Sparro >> getInvoice-reply >> Bank:HSBC

[0171]

{"bank":"Bank:HSBC","invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

[0171] --

[0171] Bank:MayBank >> payInvoice-reply >> User:XYZ Printing

[0171]

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700},"id":"ripple-2"}

[0171] XYZ finished paying invoice {

[0171] "payer": "70wqgx6",

[0171] "invoice": "6tq6wcbad",

[0171] "amount": {

[0171] "currency": "GBP",

[0172] "amount": 700

[0172] },

[0172] "id": "ripple-2"

[0172] }

[0172] ---- SWITCHING TO MODE: minimal ----

[0172] ---

[0172] Bank:HSBC >> incomingTransfer >> User:ABC Paper

[0172]

{"invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"},"transfer":{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700},"id":"ripple-2"}}

[0172] --Bank:HSBC >> createUserCode >> Sparro:Sparro

[0172] undefined

[0172] (Creating Sparro User Code - No meta-data is required.)

[0172] ---

[0172] Bank:MayBank >> createUserCode >> Sparro:Sparro

[0172] undefined

[0172] (Creating Sparro User Code - No meta-data is required.)

[0172] ---

[0172] Sparro:Sparro >> createUserCode-reply >> Bank:HSBC

[0172] {"code":"dnt7gec"}

[0172] ---

[0172] Sparro:Sparro >> createUserCode-reply >> Bank:MayBank

[0173] {"code":"6wwpwuc"}

[0173] ---

[0173] User:ABC Paper >> createInvoice >> Bank:HSBC

[0173] {"amount":{"amount":2000,"currency":"gbp"}}

[0173] ---

[0173] Bank:HSBC >> createInvoiceCode >> Sparro:Sparro

[0173] null

[0173] (Creating Invoice Code -- An invoice code is created by Sparro and connected to the bank. No invoice details are required.)

[0173] ---

[0173] Sparro:Sparro >> createInvoiceCode-reply >> Bank:HSBC

[0173] {"code":"erwkax1md"}

[0173] Bank:HSBC >> createInvoice-reply >> User:ABC Paper

[0173] {"invoice":{"amount":{"amount":2000,"currency":"gbp"},"code":"erwkax1md","payee":"User:ABC Paper","transfers":[]}}

[0173] Abc invoice { amount: { amount: 2000, currency: 'gbp' },

[0173] code: 'erwkax1md',

[0173] payee: 'User:ABC Paper',

[0173] transfers: [] }

[0173] ---

[0173] User:ABC Paper >> invoice >> User:XYZ Printing

[0174]
{"amount":{"amount":2000,"currency":"gbp"},"code":"erwkax1md","payee":"User:ABC Paper","transfers":[]}

[0174] ---
[0174] User:XYZ Printing >> payInvoice >> Bank:MayBank
[0174] {"invoice":"erwkax1md","amount":{"currency":"GBP","amount":600}}

[0174] ---
[0174] Bank:MayBank >> sendMoney >> BankGateway:MayBank
[0174]
{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600}}
[0174] ---
[0174] BankGateway:MayBank >> getInvoice >> Sparro:Sparro
[0174] "erwkax1md"
[0174] (Sending Payment to Invoice -- The payment is sent to the bank that created the invoice.)
[0174] ---
[0174] Sparro:Sparro >> getInvoice-reply >> BankGateway:MayBank
[0174] {"bank":"Bank:HSBC"}

[0174] ---
[0174] BankGateway:MayBank >> transfer >> BankGateway:HSBC
[0174]
{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}

[0174] ---
[0174] BankGateway:HSBC >> incomingTransfer >> Bank:HSBC

JPMC Ex. 1002
Page 102

[0175]

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}

[0175] ---

[0175] BankGateway:HSBC >> transfer-reply >> BankGateway:MayBank

[0175] {"success":true,"owed":{"GBP":600}}

[0175] ---

[0175] Bank:HSBC >> incomingTransfer >> User:ABC Paper

[0175]

{"invoice":{"amount":{"amount":2000,"currency":"gbp"},"code":"erwkax1md","payee":"User:ABC Paper","transfers":[{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}]},"transfer":{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}}

[0175] ---

[0175] BankGateway:MayBank >> sendMoney-reply >> Bank:MayBank

[0175]

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}

[0175] ---

[0175] Bank:MayBank >> payInvoice-reply >> User:XYZ Printing

[0175]

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}

[0175]

[0175] XYZ part-paid invoice {

[0175] "payer": "6wwpwuc",

[0176] "invoice": "erwkax1md",

[0176] "amount": {

[0176] "currency": "GBP",

[0176] "amount": 600

[0176] },

[0176] "id": "ripple-3"

[0176] }

[0176] ---

[0176] User:XYZ Printing >> payInvoice >> Bank:MayBank

[0176]

{"invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400}}

[0176] ---

[0176] Bank:MayBank >> sendMoney >> BankGateway:MayBank

[0176]

{"payer":"6wwpwue","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400}}

[0176] --

[0176] BankGateway:MayBank >> getInvoice >> Sparro:Sparro

[0176] "erwkax1md"

[0176] (Sending Payment to Invoice - The payment is sent to the bank that created the invoice.)

[0176] ---

[0176] Sparro:Sparro >> getInvoice-reply >> BankGateway:MayBank

[0176] {"bank":"Bank:HSBC"}

[0176] -

[0176] BankGateway:MayBank >> transfer >> BankGateway:HSBC

[0177]

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}

[0177] --

[0177] BankGateway:HSBC >> incomingTransfer >> Bank:HSBC

[0177]

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}

[0177] BankGateway:HSBC >> transfer-reply >> BankGateway:MayBank

[0177] {"success":true,"owed":{"GBP":2000}}

[0177] --

[0177] Bank:HSBC >> incomingTransfer >> User:ABC Paper

[0177]

{"invoice":{"amount":{"amount":2000,"currency":"gbp"},"code":"erwkax1md","payee":"User:ABC Paper","transfers":[{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"},{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}]},"transfer":{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}}

[0177] --

[0177] BankGateway:MayBank >> sendMoney-reply >> Bank:MayBank

[0177]

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}

[0178] ~~—~~

[0178] ~~Bank:MayBank >> payInvoice-reply >> User:XYZ Printing~~

[0178] ~~{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}~~

[0178] ~~XYZ finished paying invoice {~~

[0178] ~~"payer": "6wwpwuc",~~

[0178] ~~"invoice": "erwkax1md",~~

[0178] ~~"amount": {~~

[0178] ~~"currency": "GBP",~~

[0178] ~~"amount": 1400~~

[0178] ~~},~~

[0178] ~~"id": "ripple-4"~~

[0178] ~~}~~

[0179][0165]features of this embodiment include the enablement of a private, invitation only, network for banking institutions which, in a particular form, can facilitate cross-border payments thereby to enable substantially real-time payments at reduced processing cost.

[0180][0166]With reference to figure 11 there is shown a block diagram of salient characteristics of a messaging system 810 of the prior art as compared with the salient messaging characteristics of the system 1010 enabled by the code listed above and more broadly described with reference to the earlier embodiments.

[0181][0167]Figure 12 illustrates the options for data content to be included in tokens in accordance with embodiments of the invention as described above.

~~[0182]~~[0168]Figure 13 provides a comparison of characteristics of embodiments of the present invention as compared with the prior art Swift-based messaging system at a commercial layer 1270, a security layer 1271 and a technical layer 1272

~~[0183]~~[0169]Embodiments of the invention can be implemented utilising the "Ripple" the framework, protocol and gateway-or more generally any blockchain based framework. In a particular form the final settlement process can be enabled through a Ripple frame work thereby to facilitate substantially real-time settlement across multiple institutions and multiple banks.

~~[0184]~~[0170]Figure 14 is a block diagram of a further embodiment. In this instance a distributed ledger 1381 operating on blockchain principles provides for transmission of the tokenised message as for previous embodiments.

~~[0185]~~[0171]In this instance it will be observed that the tokenised transmission distributed ledger 1381 operates in parallel with conventional transmission between institution A and institution B.

~~[0186]~~[0172]Conventional transmission includes transmission of conventional messages utilising the SWIFT protocol. It is also to be noted that institution A and institution B may be subsidiaries of the same institution or may otherwise be closely related. In the alternative they may be completely independent institutions.

~~[0187]~~[0173]The tokenised message as described in previous embodiments may include information as typically transmitted by the SWIFT or other

JPMC Ex. 1002
Page 107

current acknowledged data transmission systems for transmission of financial information for the purpose of transfer of funds between parties.

~~[0188]~~[0174]The tokenised message may transmit data which includes some of the data normally included in the conventional message. In alternative forms it may include additional data. In yet alternative forms it may include data not transferred at all in the data normally included in the conventional message.

~~[0189]~~[0175]The aim, in particular forms, ultimately, is to improve the reliability of the financial transaction as between the first transacting entity and the second transacting entity and, in some forms, to provide an enhanced capability.

~~[0190]~~[0176]In the arrangement of figure 14 the data comprising the tokenised message is transmitted via nodes 1380 within a blockchain 1381.

~~[0191]~~[0177]In summary, Bank A and Bank B might be branches of the same bank, say HSBC HK and HSBC China (which today use SWIFT for intrabank transfers). So this system could be used within 1 financial institution.

~~[0192]~~[0178]In one form the purpose of storing the token only in the blockchain is really to both de-identify the information in the blockchain (which is critical for banks), and enable use of existing (SWIFT / ACH / RTGS) or new messaging systems to send the payment instruction in tokenised format. Banks today have significant investment in existing conventional messaging systems and a complete abandonment of these messaging systems would not be feasible. However settlement is still a manual process so linking the conventional messaging system to the 'blockchain' settlement system (via the token) is an important feature of this embodiment. So, in diagram 7 we

JPMC Ex. 1002
Page 108

include a SWIFT/ACH/RTGS connection between the two Financial Institutions (FIs) (or branches) for communication of the token, and the blockchain ledger is common. The data that is required to settle the payment can be provided by the FI's customer or by the FI themselves (say from a core banking system or similar).

~~[0193]~~[0179]Fig 15 illustrates in block diagram form key components of an implementation of a blockchain structure which may be utilised to implement the system of figure 14.

~~[0194]~~[0180]Each block includes verified transactions and the blockchain maintains a ledger all prior transactions. The blockchain is duplicated by all the computers on a network.

~~[0195]~~[0181]The first block in the chain is known as the Genesis block and new blocks can be added in linear and chronological order. From any given block in the chain the information of this genesis block and all blocks that led back to this one can be retrieved. A blockchain is essentially numerous blocks connected through hash chaining where each block is comprised of the following (see figure 15);

~~[0196]~~[0182]Timestamp: provides proof that the data in a block existed at a particular time;

~~[0197]~~[0183]Previous Hash: Essentially a pointer to the previous block;

~~[0198]~~[0184]Merkle Hash: Summary of all executed transactions;

~~[0199]~~[0185]Nonce: Individual blocks identity and is an arbitrary number which can only be used once.

~~[0200]~~[0186]The blockchain is managed by a network of distributed nodes where each node contains a copy of the entire blockchain. Each node in the network can add blocks to the chain, where every node is adding blocks at

the same point in the chain at the same time. The more nodes that comprise the network the harder it is to disrupt the storage of the blockchain. Unlike centralised systems which rely on a single authority, there is no single point of failure in these distributed nodes network. If you change the content of a block you change its Hash.

~~[0201]~~[0187]Blockchains can be based on/ operate in association with any one of a number of protocols – for example Ripple or Stellar.

~~[0202]~~[0188]Figure 15B shows a first step in creation of records in the block chain structure of figure 15A whilst figure 15C shows a second step in the creation of records in the chain structure of figure 15A. The chain structures of this type may be utilised in relation to the embodiments described in this application.

~~[0203]~~[0189]Figure 16 is a block diagram of a further embodiment wherein the parallel data transmission capabilities of the system are further detailed as compared with the embodiment of figure 14 .Components are numbered as for previous embodiments except in the 1400 series. So, for example, first transacting entity 1311 of the further embodiment of figure 14 becomes the first transacting entity 1411. In this instance a distributed ledger 1481 operating on blockchain principles (refer description with reference to figure 15) provides for transmission of the tokenised message as for previous embodiments.

~~[0204]~~[0190]In this instance it will be observed that the tokenised transmission distributed ledger 1481 operates in parallel with conventional transmission between institution A and institution B.

~~[0205]~~[0191]Conventional transmission includes transmission of conventional messages utilising the SWIFT protocol. It is also to be noted that institution

A 1413 and institution B 1414 may be subsidiaries of the same institution or may otherwise be closed related. In the alternative they may be completely independent institutions.

~~[0206]~~[0192]The tokenised message 1490 as described in previous embodiments may include information as typically transmitted by the SWIFT or other current acknowledged data transmission systems for transmission of financial information for the purpose of transfer of funds between parties.

~~[0207]~~[0193]The tokenised message may transmit data which includes some of the data normally included in the conventional message. In alternative forms and more particularly the form with reference to figure 16 it may include additional data however, in this instance the additional data 1491 is transmitted via blockchain 881 as an entry in a shared ledger 1492. The additional data 1491 in this instance comprises a token value 1493, a financial transaction value 1494 a sender cheque status flag 895 and a token state 1496. This entry 1497 in shared ledger 1492 can be accessed based on token value 1493. In an alternative form the entry 1497 and more particularly the token value 1493 may be secured for example requiring a separate key before the data can be accessed and/or decrypted. The data in entry 1497 may comprise deidentified data thereby to ensure that no personally identifiable information is transmitted to Bank (second intermediary entity 1414).

~~[0208]~~[0194]The aim, ultimately, is to improve the reliability of the financial transaction as between the first transacting entity and the second transacting entity and, in some forms, to provide an enhanced capability.

~~[0209]~~[0195]In particular, in preferred forms an element includes provision of systems which add additional information whereby the additional

JPMC Ex. 1002
Page 111

information is to enrich payments with more information given the inability of existing payment systems to communicate enriched information.

~~[0210]~~[0196]In the arrangement of figure 16 the data comprising the tokenised message is transmitted via nodes 1480 within a blockchain 1481.

~~[0211]~~[0197]In summary, Bank A and Bank B might be branches of the same bank, say HSBC HK and HSBC China (which today use SWIFT for intrabank transfers). So this system could be used within 1 financial institution.

~~[0212]~~[0198]In one form the purpose of storing the token only in the blockchain is really to both de-identify the information in the blockchain (which is critical for banks), and enable use of existing (SWIFT / ACH / RTGS) or new messaging systems to send the payment instruction in tokenised format. Banks today have significant investment in existing conventional messaging systems and a complete abandonment of these messaging systems would not be feasible. However settlement is still a manual process so linking the conventional messaging system to the 'blockchain' settlement system (via the token) is an important feature of this embodiment. So, in figure 16 we include a SWIFT/ACH/RTGS connection between the two Financial Institutions (FIs) (or branches) for communication of the token, and the blockchain ledger is common. The data that is required to settle the payment can be provided by the FI's customer or by the FI themselves (say from a core banking system or similar).

~~[0213]~~[0199]Figure 17 is a detailed block diagram of the system of figure 10C and figure 16.

~~[0214]~~[0200]With reference to Figure 17 there is illustrated in block diagram form a first preferred embodiment of the present invention by way of a non-

limiting example of a financial transaction. In this embodiment like components are numbered as for Figure 16 in the 1400 series.

~~[0215]~~[0201]With reference to figure 17 the financial transaction system 1010 is activated, as for the previous embodiment, when a financial transaction 1020 is entered into between at least first transacting entity 1011 and at least a second transacting entity 1012 each dealing, for the purposes of this transaction, through respective intermediary entities 1013, 1014.

~~[0216]~~[0202]At the time of and as part of entry into the financial transaction 1020 the first transacting entity 1011 accesses token database 1023 via digital device 1022 executing via a web browser interface or via execution of an application running on a portable digital devices such as a mobile telephone or in a further alternative as a point-of-sale terminal in order to arrange for the database 1023 to generate a token 1021. In this instance the token 1021 will include better data 1024 including the recipient named, BIC, IBAN, destination country, mobile number, currency, business type, communication, payment amount. In this instance the token 1021 including the metadata 1024 is stored in the token database 1023. In addition the first transacting entity 1011 communicates the token 1021 to a digital device 1030 associated with second transacting entity 1012. In this instance the communication is by way of initial transmission of the token 1021 to digital device 1022 which then on transmits the token via Internet 1031 to digital device 1030.

~~[0217]~~[0203]With reference to figure 17, when ready to settle the financial transaction 1020 the second transacting entity 1012 "logs in" to a portal associated with second intermediary entity 1014 and communicates the token 1021. In this instance have the login can be executed via a web browser associated with digital device 1030 which communicates via Internet 1031 the token 1021 to a digital processing system 1032 (including

JPMC Ex. 1002
Page 113

at least a processor and a memory) associated with second intermediary entity 1014. Substantially at the same time as part of seeking to settle the financial transaction 1020:

[~~0218~~][0204]Notification: token database 1023 notifies second intermediary entity 1014 to contact the token database 1023 from which it receives a further token 1021A.

[~~0219~~][0205]Verification: token database 1023 communicates with the processing system 1032 of second intermediary entity 1014 to verify that sufficient funds are located in account 1016 as indicated in the meta data 1024 to settle the financial transaction.

[~~0220~~][0206]Committing payer funds: payers bank debits payers account: payers bank sends notice to payer bank gateway: payers bank gateway calls token database 1023 to get approved token:

[~~0221~~][0207]Settlement: gateway of payers bank sends by way of non-limiting example XRP (the native currency of the Ripple protocol) to billers bank gateway: payers bank gateway notifies token database 1023 of receipt:

[~~0222~~][0208]Clearing: payer's bank may be a Nostro account which is debited subject to bank institution rules.

[~~0223~~][0209]Embodiments of the invention can be implemented utilising the "Ripple" framework, protocol and gateway-or more generally any blockchain based framework. In a particular form the final settlement process can be enabled through a Ripple framework thereby to facilitate substantially real-time settlement across multiple institutions and multiple banks.

~~[0224]~~[0210]With further reference to figure 17 it will be observed that the token 1021, in this instance, may be conveyed between bank 1013 and bank 1014 by way of a medium 1060 utilizing the SWIFT protocol or other compatible protocols 1050. In preferred forms the medium the medium will be an electronic communications medium and in particular forms may be implemented by way of a VPN established between bank 1013 and bank 1014.

~~[0225]~~[0211]Separately deidentified data 1051 A, B, C, D associated with the financial transaction to which the token pertains may be transmitted over a separate communication medium, in this instance internet 1031. In a preferred form the communication medium utilizes a blockchain structure as described earlier in this specification and the deidentified data 1051 A, B, C, D is located within a record structure 1061 which is replicated throughout the blockchain structure.

~~[0226]~~[0212]In use a sellers bank 1013 as part of entering into the financial transaction with buyers bank 1014 will establish a SWIFT transaction transmittable over medium 1060. Separately and preferably in parallel the sellers bank 1013 will perform associated operations needed to complete the financial transaction such as verification of the buyers ID and related characteristics. Data related to these associated operations is then placed in record structure 1061 and that record is placed into the blockchain structure. The associated data includes deidentifed data 1051 A, B, C, D.

~~[0227]~~[0213]This data is available to the buyers bank 1014 by way of the buyers bank logging into the blockchain structure and receiving the deidentified data which is associated with the financial transaction which is represented by token 1021. Thereby allowing assembly by the buyers bank 1014 of all necessary data to execute the financial transaction on behalf of the buyer and seller.

~~[0228]~~[0214]With reference to figures 16 and 17 the system provides for communication of invoice/purchase order /remittance advice information as illustrated.

~~[0229]~~[0215]It will be further observed that blockchain structures may be utilized to provide an information layer above existing legacy systems (for example based on SWIFT protocols and the like) and wherein the additional information layer provides enriched information about payments using the token. It is to be noted that existing systems do not provide enriched information and, in more particular forms, do not provide deidentified information/data for use by the communicating parties.

~~[0230]~~[0216]The above describes only some embodiments of the present invention and modifications, obvious to those skilled in the art, can be made thereto without departing from the scope of the present invention.

~~[0231]~~[0217]The computer implemented method and the system for processing a financial transaction offers a plurality of advantages. First, the invention enables a wide variety of documents to be attached to a financial transaction, by means of a token. The existing financial messaging systems allow only specific information to be attached to the financial transaction. Further, the invention enables generation of an auditable enriched data record from the documents. The enriched data record is stored in a distributed ledger (or the blockchain) and can be retrieved at any time when queried with the token. Further, the enriched data record ensures that integrity of the documents is maintained in perpetuity. Further, the documents stores enable maintaining of a state of the token. That is, a status of the financial transaction can be tracked at any time, from the respective documents stored in the document stores.

Other Exemplary Embodiments

~~[0232]~~[0218]Definitions:

~~[0233]~~[0219]Token: in this specification a "token" is a pointer to an enriched data record of a plurality data required to process a financial transaction and wherein the plurality of data is rendered, formatted or passed through an algorithm in a predetermined manner. The process of rendering, formatting or passing through an algorithm in a predetermined manner is termed "tokenisation". The tokenisation process may involve operations such as encryption and de-identification of the plurality of data.

~~[0234]~~[0220]Financial Transaction: in this specification "financial transaction" refers to a trade between two parties, for example at least a first transacting entity and a second transacting entity and wherein the trade is expressed in a financial form (for example in a Fiat currency or an electronic currency-to be distinguished, for example, from a barter transaction) which will ultimately require exchange of currency to process the financial transaction. In some instances the currency will be the same on both sides of the financial transaction. In other cases a conversion from one currency to another may be required.

~~[0235]~~[0221]Personally Identifiable Information (PII): in this specification refers to information that a regulator or privacy policy will not allow to be disclosed to a third party.

~~[0236]~~[0222]Accordingly, in one broad form of the invention, there is provided a system for settling a financial transaction electronically; said system comprising:

at least a first transacting entity;

at least a second transacting entity;

at least a first intermediary entity;

at least a second intermediary entity;

in the case where the first transacting entity enters into a financial transaction with the second transacting entity generating a tokenised message at the time of the financial transaction containing data needed to settle the financial transaction;

initiating settlement of the financial transaction by transmission of the tokenised message to the at least first transacting entity.

~~[0237]~~[0223]In a further broad form of the invention there is provided a tokenised message construction system; said system comprising:

a server in communication with a database and which facilitates communications between a plurality of parties to a financial transaction;

each party having a digitised device with which to communicate with other ones of the parties and with the server;

each party capable of generating a tokenised message via a bidirectional communication with the server.

~~[0238]~~[0224]Accordingly, in yet a further broad form of the invention there is provided tokenised message construction system; said system comprising:

a server in communication with a database and which facilitates communications between a plurality of parties to a financial transaction;

each party having a digitised device with which to communicate with other ones the parties and with the server;

each party capable of generating a tokenised message via a bidirectional communication with the server.

~~[0239]~~[0225]Preferably the tokenised message is generated with reference to a token database located at a remote location.

~~[0240]~~[0226]Preferably the tokenised message includes at least a first data element, a second data element and a third data element.

~~[0241]~~[0227]Preferably the first data element comprises identification data for a payor, the second data element comprises identification data for a payee (biller) and the third data element comprises identification currency, denomination and value data.

~~[0242]~~[0228]Preferably a further tokenised message is generated by either an intermediary entity or the token database.

~~[0243]~~[0229]Preferably a tokenised message is generated by a bi-directional communication process.

~~[0244]~~[0230]Preferably the bi-directional communication process is between the token database and an intermediary entity.

~~[0245]~~[0231]Preferably a step in producing a tokenised message involves de-identifying data.

~~[0246]~~[0232]Preferably a step in producing a tokenised message involves adding a data element to the message.

~~[0247]~~[0233]Preferably a step in producing a tokenised message involves removing a data element from the message.

~~[0248]~~[0234]Preferably a step in producing a tokenised message involves applying an algorithm to the data elements in the message.

~~[0249]~~[0235]Preferably the token database sequences the tokenised messages.

JPMC Ex. 1002
Page 119

~~[0250]~~[0236]Preferably the token database sequences the tokenised messages and transmits the tokenised messages as payment data records to a blockchain settlement system.

~~[0251]~~[0237]Preferably the blockchain settlement system employs the Ripple protocol.

~~[0252]~~[0238]Preferably the tokenised message includes at least a first data element, a second data element and a third data element.

~~[0253]~~[0239]Preferably the first data element comprises identification data for a payor, the second data element comprises identification data for a payee (biller) and the third data element comprises identification currency, denomination and value data.

~~[0254]~~[0240]Preferably a further tokenised message is generated by either an intermediary entity or the token database.

~~[0255]~~[0241]Preferably a tokenised message is generated by a bi-directional communication process.

~~[0256]~~[0242]Preferably the bi-directional communication process is between the token database and an intermediary entity.

~~[0257]~~[0243]Preferably a step in producing a tokenised message involves de-identifying data.

~~[0258]~~[0244]Preferably a step in producing a tokenised message involves adding a data element to the message.

~~[0259]~~[0245]Preferably a step in producing a tokenised message involves removing a data element from the message.

~~[0260]~~[0246]Preferably a step in producing a tokenised message involves applying an algorithm to the data elements in the message.

~~[0261]~~[0247]Preferably the token database sequences the tokenised messages.

~~[0262]~~[0248]Preferably the token database sequences the tokenised messages and transmits the tokenised messages as payment data records to a blockchain settlement system.

~~[0263]~~[0249]Preferably the blockchain settlement system employs the Ripple protocol.

~~[0264]~~[0250]Preferably a second message is transmitted between the intermediaries.

~~[0265]~~[0251]Preferably the second message is tokenised.

~~[0266]~~[0252]Preferably the second message contains conventional data.

~~[0267]~~[0253]Preferably the second message is transmitted by means of a blockchain system.

~~[0268]~~[0254]Preferably the second message includes information equivalent to that transmitted by the SWIFT system.

~~[0269]~~[0255]Preferably the tokenised message includes additional information beyond that transmitted by the SWIFT system.

JPMC Ex. 1002
Page 121

~~[0270]~~[0256]The system wherein the tokenised message includes information which verifies the security status of at least one party to the financial transaction.

~~[0271]~~[0257]Preferably the second tokenised message includes information which verifies the security status of both parties to the financial transaction.

~~[0272]~~[0258]Preferably the token is conveyed by way of a medium utilizing the SWIFT messaging system or other compatible messaging system.

~~[0273]~~[0259]Preferably the medium is implemented by way of a VPN.

~~[0274]~~[0260]Preferably deidentified data associated with the financial transaction to which the token pertains is transmitted over a separate communication medium.

~~[0275]~~[0261]Preferably the separate communication medium utilizes a blockchain structure.

~~[0276]~~[0262]Preferably the deidentified data is located within a record structure which is replicated throughout the blockchain structure.

~~[0277]~~[0263]Preferably in use a sellers bank as part of entering into the financial transaction with buyers bank will establish a SWIFT transaction.

~~[0278]~~[0264]Preferably in parallel the sellers bank will perform associated operations needed to complete the financial transaction such as verification of the buyers ID and related characteristics.

~~[0279]~~[0265]Preferably data related to the associated operations is then placed in a record structure and that record is placed into the blockchain structure.

~~[0280]~~[0266]Preferably the associated data includes deidentifed data.

~~[0281]~~[0267]Preferably the data is available to the buyers bank by way of the buyers bank logging into the blockchain structure and receiving the deidentified data which is associated with the financial transaction which is represented by the token thereby allowing assembly by the buyers bank of all necessary data to execute the financial transaction on behalf of the buyer and seller.

~~[0282]~~[0268]Preferably incorporating secure channels thereby permitting only selected entities to communicate the data to execute the financial transaction on behalf of the buyer and seller.

Advantages

~~[0283]~~[0269]The invention is not limited to interaction between two banks only, but can be extended to any number of banks involved in the financial transaction. For example, the token can be included in all the financial messages sent between a plurality of banks, and the token can be used by any bank from the plurality of banks to verify the financial transaction from the enriched data record, before taking any further steps in the process.

~~[0284]~~[0270]The messaging bus allows all the financial institutions involved in the financial transaction to communicate in real-time and ensure that the payer, the beneficiary, and all the parameters corresponding to the financial transaction are validated. Further, encryption/decryption of the requests and responses using asymmetrical pairs of keys ensures that the transmission of the request and the responses is always secure. Further, the payment risk rating ensures better straight through processing by

reducing exceptions and false positives. Also, the token is compatible with a large array of formats, including JSON, XML, CSV, SWIFT, over a number of transports, including HTTP, FTP, AMQP, and JMS.

Interpretation

~~[0285]~~[0271]Unless otherwise defined, all terms (including technical and scientific terms) used herein have the same meaning as commonly understood by one of ordinary skill in the art to which this invention belongs. It will be further understood that terms used herein should be interpreted as having a meaning that is consistent with their meaning in the context of this specification and the relevant art and will not be interpreted in an idealized or overly formal sense unless expressly so defined herein. For the purposes of the present invention, additional terms are defined below. Furthermore, all definitions, as defined and used herein, should be understood to control over dictionary definitions, definitions in documents incorporated by reference, and/or ordinary meanings of the defined terms unless there is doubt as to the meaning of a particular term, in which case the common dictionary definition and/or common usage of the term will prevail.

~~[0286]~~[0272]The terminology used herein is for the purpose of describing particular embodiments only and is not intended to be limiting of the invention. As used herein, the singular articles “a”, “an” and “the” are intended to include the plural forms as well, unless the context clearly indicates otherwise and thus are used herein to refer to one or to more than one (i.e. to “at least one”) of the grammatical object of the article. By way of example, the phrase “an element” refers to one element or more than one element.

~~[0287]~~[0273]The term “about” is used herein to refer to quantities that vary by as much as 30%, preferably by as much as 20%, and more preferably by

as much as 10% to a reference quantity. The use of the word 'about' to qualify a number is merely an express indication that the number is not to be construed as a precise value.

~~[0288]~~[0274]Throughout this specification, unless the context requires otherwise, the words "comprise", "comprises" and "comprising" will be understood to imply the inclusion of a stated step or element or group of steps or elements but not the exclusion of any other step or element or group of steps or elements.

~~[0289]~~[0275]The term "real-time" for example "displaying real-time data," refers to the display of the data without intentional delay, given the processing limitations of the system and the time required to accurately measure the data.

~~[0290]~~[0276]As used herein, the term "exemplary" is used in the sense of providing examples, as opposed to indicating quality. That is, an "exemplary embodiment" is an embodiment provided as an example, as opposed to necessarily being an embodiment of exemplary quality for example serving as a desirable model or representing the best of its kind.

~~[0291]~~[0277]The phrase "and/or," as used herein in the specification and in the claims, should be understood to mean "either or both" of the elements so conjoined, i.e., elements that are conjunctively present in some cases and disjunctively present in other cases. Multiple elements listed with "and/or" should be construed in the same fashion, i.e., "one or more" of the elements so conjoined. Other elements may optionally be present other than the elements specifically identified by the "and/or" clause, whether related or unrelated to those elements specifically identified. Thus, as a non-limiting example, a reference to "A and/or B", when used in conjunction with open-ended language such as "comprising" can refer, In one embodiment of the

invention, to A only (optionally including elements other than B); in another embodiment, to B only (optionally including elements other than A); in yet another embodiment, to both A and B (optionally including other elements); etc.

~~[0292]~~[0278]As used herein in the specification and in the claims, "or" should be understood to have the same meaning as "and/or" as defined above. For example, when separating items in a list, "or" or "and/or" shall be interpreted as being inclusive, i.e., the inclusion of at least one, but also including more than one, of a number or list of elements, and, optionally, additional unlisted items. Only terms clearly indicated to the contrary, such as "only one of" or "exactly one of," or, when used in the claims, "consisting of" will refer to the inclusion of exactly one element of a number or list of elements. In general, the term "or" as used herein shall only be interpreted as indicating exclusive alternatives (i.e. "one or the other but not both") when preceded by terms of exclusivity, such as "either," "one of," "only one of," or "exactly one of." "Consisting essentially of," when used in the claims, shall have its ordinary meaning as used in the field of patent law.

~~[0293]~~[0279]As used herein in the specification and in the claims, the phrase "at least one," in reference to a list of one or more elements, should be understood to mean at least one element selected from any one or more of the elements in the list of elements, but not necessarily including at least one of each and every element specifically listed within the list of elements and not excluding any combinations of elements in the list of elements. This definition also allows that elements may optionally be present other than the elements specifically identified within the list of elements to which the phrase "at least one" refers, whether related or unrelated to those elements specifically identified. Thus, as a non-limiting example, "at least one of A and B" (or, equivalently, "at least one of A or B," or, equivalently "at least one of A and/or B") can refer, In one embodiment of the invention, to at least

one, optionally including more than one, A, with no B present (and optionally including elements other than B); in another embodiment, to at least one, optionally including more than one, B, with no A present (and optionally including elements other than A); in yet another embodiment, to at least one, optionally including more than one, A, and at least one, optionally including more than one, B (and optionally including other elements); etc.

Bus

~~[0294]~~[0280]In the context of this document, the term "bus" and its derivatives, while being described in a preferred embodiment as being a communication bus subsystem for interconnecting various devices including by way of parallel connectivity such as Industry Standard Architecture (ISA), conventional Peripheral Component Interconnect (PCI) and the like or serial connectivity such as PCI Express (PCIe), Serial Advanced Technology Attachment (Serial ATA) and the like, should be construed broadly herein as any system for communicating data.

In accordance with:

~~[0295]~~[0281]As described herein, 'in accordance with' may also mean 'as a function of' and is not necessarily limited to the integers specified in relation thereto.

Composite items

~~[0296]~~[0282]As described herein, 'a computer implemented method' should not necessarily be inferred as being performed by a single computing device such that the steps of the computer implemented method may be performed by more than one cooperating computing devices.

~~[0297]~~[0283]Similarly objects as used herein such as 'web server', 'server', 'client computing device', 'computer readable medium' and the like should not necessarily be construed as being a single object, and may be implemented as a two or more objects in cooperation, such as, for example,

JPMC Ex. 1002
Page 127

a web server being construed as two or more web servers in a server farm cooperating to achieve a desired goal or a computer readable medium being distributed in a composite manner, such as program code being provided on a compact disk activatable by a license key downloadable from a computer network.

Database:

~~[0298]~~[0284]In the context of this document, the term "database" and its derivatives may be used to describe a single database, a set of databases, a system of databases or the like. The system of databases may comprise a set of databases wherein the set of databases may be stored on a single implementation or span across multiple implementations. The term "database" is also not limited to refer to a certain database format rather may refer to any database format. For example, database formats may include MySQL, MySQLi , XML or the like.

Wireless:

~~[0299]~~[0285]The invention may be embodied using devices conforming to other network standards and for other applications, including, for example other WLAN standards and other wireless standards. Applications that can be accommodated include IEEE 802.11 wireless LANs and links, and wireless Ethernet.

~~[0300]~~[0286]In the context of this document, the term "wireless" and its derivatives may be used to describe circuits, devices, systems, methods, techniques, communications channels, etc., that may communicate data through the use of modulated electromagnetic radiation through a non-solid medium. The term does not imply that the associated devices do not contain any wires, although in some embodiments they might not. In the context of this document, the term "wired" and its derivatives may be used to describe circuits, devices, systems, methods, techniques, communications channels, etc., that may communicate data through the

JPMC Ex. 1002
Page 128

use of modulated electromagnetic radiation through a solid medium. The term does not imply that the associated devices are coupled by electrically conductive wires.

Processes:

~~[0301]~~[0287]Unless specifically stated otherwise, as apparent from the following discussions, it is appreciated that throughout the specification discussions utilizing terms such as "processing", "computing", "calculating", "determining", "analysing" or the like, refer to the action and/or processes of a computer or computing system, or similar electronic computing device, that manipulate and/or transform data represented as physical, such as electronic, quantities into other data similarly represented as physical quantities.

Processor:

~~[0302]~~[0288]In a similar manner, the term "processor" may refer to any device or portion of a device that processes electronic data, e.g., from registers and/or memory to transform that electronic data into other electronic data that, e.g., may be stored in registers and/or memory. A "computer" or a "computing device" or a "computing machine" or a "computing platform" may include one or more processors.

~~[0303]~~[0289]The computer implemented methodologies described herein are, In one embodiment of the invention, performable by one or more processors that accept computer-readable (also called machine-readable) code containing a set of instructions that when executed by one or more of the processors carry out at least one of the computer implemented methods described herein. Any processor capable of executing a set of instructions (sequential or otherwise) that specify actions to be taken are included. Thus, one example is a typical processing system that includes one or more processors. The processing system further may include a memory subsystem including main RAM and/or a static RAM, and/or ROM.

Computer-Readable Medium:

~~[0304]~~[0290]Furthermore, a computer-readable carrier medium may form, or be included in a computer program product. A computer program product can be stored on a computer usable carrier medium, the computer program product comprising a computer readable program means for causing a processor to perform a method as described herein.

Networked or Multiple Processors:

~~[0305]~~[0291]In alternative embodiments, the one or more processors operate as a standalone device or may be connected, e.g., networked to other processor(s), in a networked deployment, the one or more processors may operate in the capacity of a server or a client machine in server-client network environment, or as a peer machine in a peer-to-peer or distributed network environment. The one or more processors may form a web appliance, a network router, switch or bridge, or any machine capable of executing a set of instructions (sequential or otherwise) that specify actions to be taken by that machine.

~~[0306]~~[0292]Note that while some diagram(s) only show(s) a single processor and a single memory that carries the computer-readable code, those in the art will understand that many of the components described above are included, but not explicitly shown or described in order not to obscure the inventive aspect. For example, while only a single machine is illustrated, the term "machine" shall also be taken to include any collection of machines that individually or jointly execute a set (or multiple sets) of instructions to perform any one or more of the computer implemented methodologies discussed herein.

Additional Embodiments:

~~[0307]~~[0293]Thus, one embodiment of each of the computer implemented methods described herein is in the form of a computer-readable carrier

medium carrying a set of instructions, e.g., a computer program that are for execution on one or more processors. Thus, as will be appreciated by those skilled in the art, embodiments of the present invention may be embodied as a method, an apparatus such as a special purpose apparatus, an apparatus such as a data processing system, or a computer-readable carrier medium. The computer-readable carrier medium carries computer readable code including a set of instructions that when executed on one or more processors cause a processor or processors to implement a method. Accordingly, aspects of the present invention may take the form of a method, an entirely hardware embodiment, an entirely software embodiment or an embodiment combining software and hardware aspects. Furthermore, the present invention may take the form of carrier medium (e.g., a computer program product on a computer-readable storage medium) carrying computer-readable program code embodied in the medium.

Carrier Medium:

~~[0308]~~[0294]The software may further be transmitted or received over a network via a network interface device. While the carrier medium is shown in an example embodiment to be a single medium, the term "carrier medium" should be taken to include a single medium or multiple media (e.g., a centralized or distributed database, and/or associated caches and servers) that store the one or more sets of instructions. The term "carrier medium" shall also be taken to include any medium that is capable of storing, encoding or carrying a set of instructions for execution by one or more of the processors and that cause the one or more processors to perform any one or more of the computer implemented methodologies of the present invention. A carrier medium may take many forms, including but not limited to, non-volatile media, volatile media, and transmission media.

Implementation:

~~[0309]~~[0295]It will be understood that the steps of methods discussed are performed In one embodiment of the invention by an appropriate processor (or processors) of a processing (i.e., computer) system executing instructions (computer-readable code) stored in storage. It will also be understood that the invention is not limited to any particular implementation or programming technique and that the invention may be implemented using any appropriate techniques for implementing the functionality described herein. The invention is not limited to any particular programming language or operating system.

Means For Carrying out a Method or Function

~~[0310]~~[0296]Furthermore, some of the embodiments are described herein as a method or combination of elements of a method that can be implemented by a processor of a processor device, computer system, or by other means of carrying out the function. Thus, a processor with the necessary instructions for carrying out such a method or element of a method forms a means for carrying out the computer implemented method or element of a method. Furthermore, an element described herein of an apparatus embodiment is an example of a means for carrying out the function performed by the element for the purpose of carrying out the invention.

Connected

~~[0311]~~[0297]Similarly, it is to be noticed that the term connected, when used in the claims, should not be interpreted as being limitative to direct connections only. Thus, the scope of the expression a device A connected to a device B should not be limited to devices or systems wherein an output of device A is directly connected to an input of device B. It means that there exists a path between an output of A and an input of B which may be a path including other devices or means. "Connected" may mean that two or more elements are either in direct physical or electrical contact, or that two or

more elements are not in direct contact with each other but yet still co-operate or interact with each other.

Embodiments:

~~[0312]~~[0298]Reference throughout this specification to "one embodiment" or "an embodiment" means that a particular feature, structure or characteristic described in connection with the embodiment is included in at least one embodiment of the present invention. Thus, appearances of the phrases "In one embodiment of the invention" or "in an embodiment" in various places throughout this specification are not necessarily all referring to the same embodiment, but may. Furthermore, the particular features, structures or characteristics may be combined in any suitable manner, as would be apparent to one of ordinary skill in the art from this disclosure, in one or more embodiments.

~~[0313]~~[0299]Similarly it should be appreciated that in the above description of example embodiments of the invention, various features of the invention are sometimes grouped together in a single embodiment, figure, or description thereof for the purpose of streamlining the disclosure and aiding in the understanding of one or more of the various inventive aspects. This method of disclosure, however, is not to be interpreted as reflecting an intention that the claimed invention requires more features than are expressly recited in each claim. Rather, as the following claims reflect, inventive aspects lie in less than all features of a single foregoing disclosed embodiment. Thus, the claims following the Detailed Description of Specific Embodiments are hereby expressly incorporated into this Detailed Description of Specific Embodiments, with each claim standing on its own as a separate embodiment of this invention.

~~[0314]~~[0300]Furthermore, while some embodiments described herein include some but not other features included in other embodiments, combinations

of features of different embodiments are meant to be within the scope of the invention, and form different embodiments, as would be understood by those in the art. For example, in the following claims, any of the claimed embodiments can be used in any combination.

Specific Details

~~[0315]~~[0301]In the description provided herein, numerous specific details are set forth. However, it is understood that embodiments of the invention may be practiced without these specific details. In other instances, well-known methods, structures and techniques have not been shown in detail in order not to obscure an understanding of this description.

~~[0316]~~[0302]It will be appreciated that the computer implemented methods and systems described/illustrated above at least substantially provides a manner in which data generated in an EHR, during an episode of care, may be de-identified (or anonymized) and provided to a user through a secure channel.

~~[0317]~~[0303]The embodiments described herein, and/or shown in the drawings, are presented by way of example only and are not limiting as to the scope of the invention. Unless otherwise specifically stated, individual aspects and components of the embodiments may be modified, or may have been substituted therefore known equivalents, or as yet unknown substitutes such as may be developed in the future or such as may be found to be acceptable substitutes in the future. The embodiments may also be modified for a variety of applications while remaining within the scope and spirit of the claimed invention, since the range of potential applications is great, and since it is intended that the present invention be adaptable to many such variations.

Different Instances of Objects

~~[0318]~~[0304]As used herein, unless otherwise specified the use of the ordinal adjectives "first", "second", "third", etc., to describe a common object, merely indicate that different instances of like objects are being referred to, and are not intended to imply that the objects so described must be in a given sequence, either temporally, spatially, in ranking, or in any other manner.

Comprising and Including

~~[0319]~~[0305]In the claims which follow and in the preceding description of the invention, except where the context requires otherwise due to express language or necessary implication, the word "comprise" or variations such as "comprises" or "comprising" are used in an inclusive sense, i.e. to specify the presence of the stated features but not to preclude the presence or addition of further features in various embodiments of the invention.

~~[0320]~~[0306]Any one of the terms: including or which includes or that includes as used herein is also an open term that also means including at least the elements/features that follow the term, but not excluding others. Thus, including is synonymous with and means comprising.

Scope of Invention

~~[0321]~~[0307]Thus, while there has been described what are believed to be the preferred embodiments of the invention, those skilled in the art will recognize that other and further modifications may be made thereto without departing from the spirit of the invention, and it is intended to claim all such changes and modifications as fall within the scope of the invention. For example, any formulas given above are merely representative of procedures that may be used. Functionality may be added or deleted from the block diagrams and operations may be interchanged among functional blocks. Steps may be added or deleted to methods described within the scope of the present invention.

JPMC Ex. 1002
Page 135

~~[0322]~~[0308]Although the invention has been described with reference to specific examples, it will be appreciated by those skilled in the art that the invention may be embodied in many other forms.

Chronological order

~~[0323]~~[0309]For the purpose of this specification, where method steps are described in sequence, the sequence does not necessarily mean that the steps are to be carried out in chronological order in that sequence, unless there is no other logical manner of interpreting the sequence.

Industrial Applicability

~~[0324]~~[0310]It is apparent from the above, that the arrangements described are applicable to the industries dealing with banking, brokerages, insurance companies, investment companies and Unit Investment Trusts (UIT) etc.

Examples of tokenised messages and their generation and transmission

The previous, meta-data mode is first. It switches to minimal half way through

--

Bank:HSBC >> createUserCode >> Sparro:Sparro

{"id":"User:ABC Paper","name":"ABC Paper"}

(Creating Sparro User Code - Meta-data given can be used by other banks for compliance and for confirming payee with customers.)

--

Bank:MayBank >> createUserCode >> Sparro:Sparro

{"id":"User:XYZ Printing","name":"XYZ Printing"}

(Creating Sparro User Code - Meta-data given can be used by other banks for compliance and for confirming payee with customers.)

--

Sparro:Sparro >> createUserCode-reply >> Bank:HSBC

{"id":"User:ABC Paper","name":"ABC Paper","code":"65q3gdd"}

--

Sparro:Sparro >> createUserCode-reply >> Bank:MayBank

{"id":"User:XYZ Printing","name":"XYZ Printing","code":"70wqgx6"}

--

User:ABC Paper >> createInvoice >> Bank:HSBC

{"amount":{"amount":1000,"currency":"gbp"}}

--

Bank:HSBC >> createInvoiceCode >> Sparro:Sparro

{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd"}

(Creating Invoice Code - An invoice code is created by Sparro and connected to the bank.)

-

Sparro:Sparro >> createInvoiceCode-reply >> Bank:HSBC

{"code":"6tq6wcbad"}

--

Bank:HSBC >> createInvoice-reply >> User:ABC Paper
{"invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":
"65q3gdd","code":"6tq6wcbad"}}

Abc invoice { amount: { amount: 1000, currency: 'gbp' },
payee: '65q3gdd',
code: '6tq6wcbad' }
--
User:ABC Paper >> invoice >> User:XYZ Printing
{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":
"6tq6wcbad"}
-
User:XYZ Printing >> payInvoice >> Bank:MayBank
{"invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300}}
--
Bank:MayBank >> sendMoney >> BankGateway:MayBank
{"payer":"70wgqx6","invoice":"6tq6wcbad","amount":{"currency":"GBP",
"amount":300}}
--
BankGateway:MayBank >> getInvoice >> Sparro:Sparro
"6tq6wcbad"
(Sending Payment to Invoice - The payment is sent to the bank
that created the invoice.)
--
Sparro:Sparro >> getInvoice-reply >> BankGateway:MayBank
{"bank":"Bank:HSBC","invoice":{"amount":{"amount":1000,"currency":
"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}
--
BankGateway:MayBank >> transfer >> BankGateway:HSBC
{"payer":"70wgqx6","invoice":"6tq6wcbad","amount":{"currency":"GBP",
"amount":300},"id":"ripple-1"}

--
BankGateway:HSBC >> incomingTransfer >> Bank:HSBC
{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":"ripple-1"}
--
BankGateway:HSBC >> transfer-reply >> BankGateway:MayBank
{"success":true,"owed":{"GBP":300}}
--
Bank:HSBC >> getInvoice >> Sparro:Sparro
"6tq6wcbad"
--
BankGateway:MayBank >> sendMoney-reply >> Bank:MayBank
{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":"ripple-1"}
--
Sparro:Sparro >> getInvoice-reply >> Bank:HSBC
{"bank":"Bank:HSBC","invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}
--
Bank:MayBank >> payInvoice-reply >> User:XYZ Printing
{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":"ripple-1"}

XYZ part-paid invoice {
"payer": "70wqgx6",
"invoice": "6tq6wcbad",
"amount": {
"currency": "GBP",
"amount": 300
},
"id": "ripple-1"

--

Bank:HSBC >> incomingTransfer >> User:ABC Paper

{"invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":
"65q3gdd","code":"6tq6wcbad"},"transfer":{"payer":"70wqgx6","invoice":
"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":"ripple-1"}}

--

User:XYZ Printing >> payInvoice >> Bank:MayBank

{"invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700}}

--

Bank:MayBank >> sendMoney >> BankGateway:MayBank

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP",
"amount":700}}

--

BankGateway:MayBank >> getInvoice >> Sparro:Sparro

"6tq6wcbad"

(Sending Payment to Invoice - The payment is sent to the bank
that created the invoice.)

--

Sparro:Sparro >> getInvoice-reply >> BankGateway:MayBank

{"bank":"Bank:HSBC","invoice":{"amount":{"amount":1000,
"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

--

BankGateway:MayBank >> transfer >> BankGateway:HSBC

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":
{"currency":"GBP","amount":700},"id":"ripple-2"}

--

BankGateway:HSBC >> incomingTransfer >> Bank:HSBC

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":
{"currency":"GBP","amount":700},"id":"ripple-2"}

--

BankGateway:HSBC >> transfer-reply >> BankGateway:MayBank

{"success":true,"owed":{"GBP":1000}}

--

Bank:HSBC >> getInvoice >> Sparro:Sparro

"6tq6wcbad"

-

BankGateway:MayBank >> sendMoney-reply >> Bank:MayBank

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":
{"currency":"GBP","amount":700},"id":"ripple-2"}

--

Sparro:Sparro >> getInvoice-reply >> Bank:HSBC

{"bank":"Bank:HSBC","invoice":{"amount":{"amount":
1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

--

Bank:MayBank >> payInvoice-reply >> User:XYZ Printing

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":
{"currency":"GBP","amount":700},"id":"ripple-2"}

XYZ finished paying invoice {

"payer": "70wqgx6",

"invoice": "6tq6wcbad",

"amount": {

"currency": "GBP",

"amount": 700

},

"id": "ripple-2"

}

--- SWITCHING TO MODE: minimal ---

--

Bank:HSBC >> incomingTransfer >> User:ABC Paper

{"invoice":{"amount":{"amount":1000,"currency":"gbp"},
"payee":"65q3gdd","code":"6tq6wcbad"},"transfer":
{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":

{"currency":"GBP","amount":700},"id":"ripple-2"}}
--Bank:HSBC >> createUserCode >> Sparro:Sparro
undefined
(Creating Sparro User Code - No meta-data is required.)
--
Bank:MayBank >> createUserCode >> Sparro:Sparro
undefined
(Creating Sparro User Code - No meta-data is required.)
--
Sparro:Sparro >> createUserCode-reply >> Bank:HSBC
{"code":"dnt7gec"}
--
Sparro:Sparro >> createUserCode-reply >> Bank:MayBank
{"code":"6wwpwuc"}
--
User:ABC Paper >> createInvoice >> Bank:HSBC
{"amount":{"amount":2000,"currency":"gbp"}}
--
Bank:HSBC >> createInvoiceCode >> Sparro:Sparro
null
(Creating Invoice Code - An invoice code is created by Sparro
and connected to the bank. No invoice details are required.)
--
Sparro:Sparro >> createInvoiceCode-reply >> Bank:HSBC
{"code":"erwkax1md"}
--Bank:HSBC >> createInvoice-reply >> User:ABC Paper
{"invoice":{"amount":{"amount":2000,"currency":"gbp"},
"code":"erwkax1md","payee":"User:ABC Paper","transfers":[]}}
Abc invoice { amount: { amount: 2000, currency: 'gbp' },
code: 'erwkax1md',
payee: 'User:ABC Paper',

transfers: [] }

--

User:ABC Paper >> invoice >> User:XYZ Printing

{"amount":{"amount":2000,"currency":"gbp"},"code":
"erwkax1md","payee":"User:ABC Paper","transfers":[]}

--

User:XYZ Printing >> payInvoice >> Bank:MayBank

{"invoice":"erwkax1md","amount":{"currency":"GBP","amount":600}}

--

Bank:MayBank >> sendMoney >> BankGateway:MayBank

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":
{"currency":"GBP","amount":600}}

--

BankGateway:MayBank >> getInvoice >> Sparro:Sparro

"erwkax1md"

(Sending Payment to Invoice - The payment is sent to the bank
that created the invoice.)

--

Sparro:Sparro >> getInvoice-reply >> BankGateway:MayBank

{"bank":"Bank:HSBC"}

--

BankGateway:MayBank >> transfer >> BankGateway:HSBC

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":
{"currency":"GBP","amount":600},"id":"ripple-3"}

--

BankGateway:HSBC >> incomingTransfer >> Bank:HSBC

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":
{"currency":"GBP","amount":600},"id":"ripple-3"}

--

BankGateway:HSBC >> transfer-reply >> BankGateway:MayBank

{"success":true,"owed":{"GBP":600}}

--

Bank:HSBC >> incomingTransfer >> User:ABC Paper

{"invoice":{"amount":{"amount":2000,"currency":"gbp"},"code":
"erwkax1md","payee":"User:ABC
Paper","transfers":[{"payer":"6wwpwuc","invoice":
"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-
3"}]},"transfer":{"payer":"6wwpwuc","invoice":"erwkax1md",
"amount":{"currency":"GBP","amount":600},"id":"ripple-3"}}

--

BankGateway:MayBank >> sendMoney-reply >> Bank:MayBank

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":
{"currency":"GBP","amount":600},"id":"ripple-3"}

--

Bank:MayBank >> payInvoice-reply >> User:XYZ Printing

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":
{"currency":"GBP","amount":600},"id":"ripple-3"}

XYZ part-paid invoice {

"payer": "6wwpwuc",

"invoice": "erwkax1md",

"amount": {

"currency": "GBP",

"amount": 600

},

"id": "ripple-3"

}

--

User:XYZ Printing >> payInvoice >> Bank:MayBank

{"invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400}}

--

Bank:MayBank >> sendMoney >> BankGateway:MayBank

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":

{"currency":"GBP","amount":1400}}

--

BankGateway:MayBank >> getInvoice >> Sparro:Sparro

"erwkax1md"

(Sending Payment to Invoice - The payment is sent to the bank that created the invoice.)

--

Sparro:Sparro >> getInvoice-reply >> BankGateway:MayBank

{"bank":"Bank:HSBC"}

--

BankGateway:MayBank >> transfer >> BankGateway:HSBC

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}

--

BankGateway:HSBC >> incomingTransfer >> Bank:HSBC

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}

BankGateway:HSBC >> transfer-reply >> BankGateway:MayBank

{"success":true,"owed":{"GBP":2000}}

--

Bank:HSBC >> incomingTransfer >> User:ABC Paper

{"invoice":{"amount":{"amount":2000,"currency":"gbp"},"code":"erwkax1md","payee":"User:ABC Paper","transfers":[{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"},{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}]},"transfer":{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}}

--

BankGateway:MayBank >> sendMoney-reply >> Bank:MayBank

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":
{"currency":"GBP","amount":1400},"id":"ripple-4"}

--

Bank:MayBank >> payInvoice-reply >> User:XYZ Printing

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":
{"currency":"GBP","amount":1400},"id":"ripple-4"}

XYZ finished paying invoice {

"payer": "6wwpwuc",
"invoice": "erwkax1md",
"amount": {
"currency": "GBP",
"amount": 1400
},
"id": "ripple-4"

}

COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR

[001] This application is the U.S. national phase of International Application No. PCT/AU2016/000279 filed August 12, 2016 which designated the U.S. and claims priority to Australian Patent Application No. 2015903292 filed August 14, 2015, Australian Patent Application No. 2016900239 filed January 27, 2016, and Australian Patent Application No. 2016901924 filed May 20, 2016, the entire contents of each of which are hereby incorporated by reference.

Field of the Invention

[002] The present invention relates to financial transactions and in particular to a method and a system for processing a financial transaction.

[003] The invention has been developed primarily for use in/with financial transactions and will be described hereinafter with reference to this application. However, it will be appreciated that the invention is not limited to this particular field of use.

Background of the Invention

[004] A financial transaction comprises at least two parties, with a transfer of currency taking place between the two parties. The currency may include electronic currency and fiat currency. In either case, any financial transaction includes a plurality of data associated with the financial transaction. The plurality of data may include payment metadata such as account numbers of the at least two parties, Business Identifier Codes (BIC) of the financial institutions corresponding to the at least two parties, amount of currency to be transferred and type of currency etc. Further, the plurality of data may include regulatory compliance documents such as KYC documents.

[005] Generally, it is difficult to keep track of the plurality of data during the financial transaction. Further, it is even more difficult to ensure that integrity of the plurality of data is maintained either during or after the financial transaction has been completed or to evidence that it existed at a certain point in the financial transaction process. Many settlement systems are characterised by effective one-way transmission of the plurality of data in any given financial transaction (for example systems based on SWIFT messaging). If it is subsequently discovered that there are deficiencies in the plurality of data transmitted, time consuming checking and querying operations and correspondence often ensues before the financial transaction can be effected.

[006] Therefore there remains, in the art, a need for improved methods and systems for processing a financial transaction which do not suffer from the above mentioned issues.

[007] Any discussion of the background art throughout the specification should in no way be considered as an admission that such background art is prior art, nor that such background art is widely known or forms part of the common general knowledge in the field in Australia or any other country.

Summary of the Invention

[008] According to a first aspect of the present invention, there is provided a computer implemented method for processing a financial transaction, the method comprising the steps of transmitting one or more documents pertaining to the financial transaction, from a first intermediary server to a first document store, generating an enriched data record from the one or more documents, at the first intermediary server, and adding the enriched data record into a blockchain, from the first intermediary sever, requesting generation of a token corresponding to the financial transaction, to a token server, from the first intermediary server, via a messaging bus, generating

the token at the token server and adding the token into the blockchain from the token server, transmitting the token to the first intermediary server from the token server, via the messaging bus and transmitting the token from the first intermediary server to the first document store. The token provides a pointer to the enriched data record in the blockchain. Thus the token can used to retrieve the enriched data record at a time of an audit.

[009] In one embodiment of the invention, the computer implemented method further comprises the step of sending a first financial message comprising the token, from the first intermediary server to a second intermediary server, indicative of making a payment to a second user.

[010] In one embodiment of the invention, the computer implemented method further comprises the steps of implementing a smart contract at the token server; and adding the smart contract into the blockchain, from the token server.

[011] In one embodiment of the invention, the computer implemented method further comprises the steps of transmitting the token from the first intermediary server to a first digital device available with a first user, providing the token to a second user, by the first user, providing the token to a second intermediary server, from the second digital device, transmitting the token to a second document store, from the second intermediary server and sending a second financial message comprising the token, from the second intermediary server to the first intermediary server, indicative of making a payment to the first user.

[012] In one embodiment of the invention, the step of generating the enriched data record comprises extracting a plurality of attributes from the one or more documents, at the first intermediary server and combining the plurality

of attributes to generate the enriched data record, at the first intermediary server.

[013] In one embodiment of the invention, the step of generating the enriched data record comprises extracting a plurality of attributes from the one or more documents, at the first intermediary server, de-identifying the plurality of attributes to obtain a plurality of de-identified attributes, at the first intermediary server and combining the plurality of de-identified attributes to generate the enriched data record, at the first intermediary server. De-identification of the plurality of attributes ensures that confidentiality of any person or entity involved in the financial transaction is not compromised during a hacking attack on the blockchain.

[014] In one embodiment of the invention, the step of generating the enriched data record comprises extracting a plurality of attributes from the one or more documents, at the first intermediary server, hashing the plurality of attributes to generate a plurality of respective hashes, at the first intermediary server and combining the plurality of hashes to generate the enriched data record, at the first intermediary server. Hashing provides even more protection against tampering of theft, to the one or more documents, as the hashes are irreversible.

[015] In one embodiment of the invention, the computer implemented method further comprises the step of assigning a payment risk rating to the token. The payment risk rating is a direct measure of the regulatory and other compliance checks involved in the financial transaction.

[016] In one embodiment of the invention, the computer implemented method further comprises the steps of transmitting one or more first requests, each comprising the token, from the first intermediary server to the second

intermediary server, via the messaging bus, receiving the one or more first requests at the second intermediary server and transmitting the one or more first requests and the token from the second intermediary server to a second document store, generating one or more first responses, each comprising the token, corresponding to the respective one or more first requests, at the second intermediary server, transmitting the one or more first responses from the second intermediary server to the first intermediary server, via the messaging bus, hashing the one or more first requests and the one or more first responses at the second intermediary server to generate one or more first request hashes and one or more first response hashes, respectively, adding the one or more first request hashes and the one or more first response hashes to the enriched data record in the blockchain, from the second intermediary server and receiving the one or more first responses at the first intermediary server and transmitting the one or more first responses to the first document store. This communication between the first intermediary server and the second intermediary server allows the first intermediary server to execute all the necessary compliance checks.

[017] In one embodiment of the invention, the computer implemented method further comprises the steps of hashing the one or more first responses at the first intermediary server to regenerate the one or more first response hashes and verifying the one or more first response hashes with the blockchain from the first intermediary server, using the token. Thus, the integrity of the one or more first responses can be verified with the blockchain, at any given time.

[018] In one embodiment of the invention, each one of the one or more first requests are encrypted with a second public key and signed with a first public key at the first intermediary server, before transmission to the second intermediary server and decrypted with a second private key at the second

intermediary server after reception from the first intermediary server. Further, each one of the one or more first responses are encrypted with the first public key and signed with the second public key at the second intermediary server, before transmission to the first intermediary server and decrypted with a first private key at the first intermediary server after reception from the second intermediary server. Using pairs of asymmetrical keys ensures that the requests and the responses are not intercepted during transmission.

[019] In one embodiment of the invention, the one or more first responses comprise one or more second regulatory compliance documents pertaining to a second user.

[020] In one embodiment of the invention, the computer implemented method further comprises the steps of transmitting one or more second requests, each comprising the token, from the second intermediary server to the first intermediary server, via the messaging bus, receiving the one or more second requests at the first intermediary server and transmitting the one or more second requests from the first intermediary server to the first document store, generating one or more second responses, each comprising the token, corresponding to the respective one or more second requests, at the first intermediary server, transmitting the one or more second responses from the first intermediary server to the second intermediary server, via the messaging bus, hashing the one or more second requests and the one or more second responses at the first intermediary server to generate one or more second request hashes and one or more second response hashes, respectively, adding the one or more second request hashes and the one or more second response hashes to the enriched data record in the blockchain, from the first intermediary server and receiving the one or more second responses at the second intermediary

server and transmitting the one or more second responses to the second document store. This communication enables the second intermediary server to execute all the necessary compliance checks.

[021] In one embodiment of the invention, the computer implemented method further comprises the steps of hashing the one or more second responses at the second intermediary server to regenerate the one or more second response hashes and verifying the one or more second response hashes with the blockchain from the second intermediary server, using the token. Similar to one or more first responses, the integrity of the one or more second responses can be verified with the blockchain, at any given time.

[022] In one embodiment of the invention, each one of the one or more second requests are encrypted with a first public key and signed with a second public key at the second intermediary server, before transmission to the first intermediary server and decrypted with a first private key at the first intermediary server after reception from the second intermediary server. Further, each one of the one or more second responses are encrypted with the second public key and signed with the first public key at the first intermediary server, before transmission to the second intermediary server and decrypted with a second private key at the second intermediary server after reception from the first intermediary server. Using pairs of asymmetrical keys ensures that the requests and the responses are not intercepted during transmission.

[023] In one embodiment of the invention, the computer implemented method further comprises the steps of adding the first public key from the first intermediary server into the blockchain and adding the second public key from the second intermediary server into the blockchain.

[024] In one embodiment of the invention, the one or more second responses comprise one or more first regulatory compliance documents pertaining to a first user.

[025] According to a second aspect of the present invention, there is provided a system for processing a financial transaction, the system comprising a first intermediary server operably connected to a network and a first document store, a token server operably connected to the network, a messaging bus operably connected to the network and a blockchain operably connected to the network. Further, the first intermediary server is configured to transmit one or more documents pertaining to the financial transaction, to the first document store, generate an enriched data record from the one or more documents and add the enriched data record into the blockchain, request generation of a token corresponding to the financial transaction, to the token server, via the messaging bus and transmit the token to the first document store. Further, the token server is configured to generate the token and add the token into the blockchain and transmit the token to the first intermediary server, via the messaging bus.

[026] In one embodiment of the invention, the system further comprises a second intermediary server operably connected to the network and a second document store. Further, the first intermediary server is further configured to send a first financial message comprising the token, to the second intermediary server, indicative of making a payment to a second user.

[027] In one embodiment of the invention, the token server is further configured to implement a smart contract and add the smart contract into the blockchain.

[028] In one embodiment of the invention, the system further comprises a first digital device operably connected to the network, a second digital device operably connected to the network, a second intermediary server operably connected to the network and a second document store. Further, the first intermediary server is further configured to transmit the token to the first digital device. Further, the first digital device comprises a first memory and a first processor operably connected to the first memory, the first memory comprising a first computer program code, the first computer program code when executed by the first processor, instructs the first processor to receive the token from the first intermediary server, provide the token to the second digital device. Further, the second digital device comprises a second memory and a second processor operably connected to the second memory, the second memory comprising a second computer program code, the second computer program code when executed by the second processor, instructs the second processor to receive the token from the first digital device and provide the token to the second intermediary server. Also, the second intermediary server is configured to receive the token from the second digital device, transmit the token to the second document store and send a second financial message comprising the token, to the first intermediary server, indicative of making a payment to a first user.

[029] In one embodiment of the invention, for generation of the enriched data record, the first intermediary server is configured to extract a plurality of attributes from the one or more documents and combine the plurality of attributes to generate the enriched data record.

[030] In one embodiment of the invention, for generation of the enriched data record, the first intermediary server is configured to extract a plurality of attributes from the one or more documents, de-identify the plurality of

attributes to obtain a plurality of de-identified attributes and combine the plurality of de-identified attributes to generate the enriched data record.

[031] In one embodiment of the invention, for generation of the enriched data record, the first intermediary server is configured to extract a plurality of attributes from the one or more documents, hash the plurality of attributes to generate a plurality of respective hashes and combine the plurality of hashes to generate the enriched data record.

[032] In one embodiment of the invention, the first intermediary server is further configured to assign a payment risk rating to the token.

[033] In one embodiment of the invention, the system further comprises a second intermediary server operably connected to the network and a second document store. Further, the first intermediary server is configured to transmit one or more first requests, each comprising the token, to the second intermediary server, via the messaging bus and receive one or more first responses and transmit the one or more first responses to the first document store. Further, the second intermediary server is configured to receive the one or more first requests from the first intermediary server and transmit the one or more first requests and the token to the second document store, generate the one or more first responses, each comprising the token, corresponding to the respective one or more first requests, transmit the one or more first responses to the first intermediary server, via the messaging bus, hash the one or more first requests and the one or more first responses to generate one or more first request hashes and one or more first response hashes, respectively and add the one or more first request hashes and the one or more first response hashes to the enriched data record in the blockchain.

[034] In one embodiment of the invention, the first intermediary server is further configured to hash the one or more first responses to regenerate the one or more first response hashes and verify the one or more first response hashes with the blockchain, using the token.

[035] In one embodiment of the invention, the first intermediary server is further configured to encrypt each one of the one or more first requests with a second public key and sign each one of the one or more first requests with a first public key, before transmission to the second intermediary server and decrypt each one of the one or more first responses with a first private key after reception from the second intermediary server. Further, the second intermediary server is further configured to encrypt the each one of the one or more first responses with the first public key and sign the each one of the one or more first responses with the second public key, before transmission to the first intermediary server and decrypt the each one of the one or more first requests with a second private key after reception from the first intermediary server.

[036] In one embodiment of the invention, the one or more first responses comprise one or more second regulatory compliance documents pertaining to a second user.

[037] In one embodiment of the invention, the system further comprises a second intermediary server connected to the network and a second document store. Further, the second intermediary server is configured to transmit one or more second requests, each comprising the token, to the first intermediary server, via the messaging bus, receive one or more second responses and transmit the one or more second responses to the second document store. Further, the first intermediary server is further configured to receive the one or more second requests and transmit the one

or more second requests to the first document store, generate the one or more second responses, each comprising the token, corresponding to the respective one or more second requests, transmit the one or more second responses to the second intermediary server, via the messaging bus, hash the one or more second requests and the one or more second responses to generate one or more second request hashes and one or more second response hashes, respectively and add the one or more second request hashes and the one or more second response hashes to the enriched data record in the blockchain.

[038] In one embodiment of the invention, the second intermediary server is further configured to hash the one or more second responses to regenerate the one or more second response hashes and verify the one or more second response hashes with the blockchain, using the token.

[039] In one embodiment of the invention, the second intermediary server is further configured to encrypt each one of the one or more second requests with a first public key and sign each one of the one or more second requests with a second public key, before transmission to the first intermediary server and decrypt each one of the one or more second responses with a second private key after reception from the first intermediary server. Further, the first intermediary server is further configured to encrypt the each one of the one or more second responses with the second public key and sign the each one of the one or more second responses with the first public key, before transmission to the second intermediary server and decrypt the each one of the one or more second requests with a first private key after reception from the second intermediary server.

[040] In one embodiment of the invention, the first intermediary server is further configured to add the first public key into the blockchain and the

second intermediary server is further configured to add the second public key into the blockchain.

[041] In one embodiment of the invention, the one or more second responses comprise one or more first regulatory compliance documents pertaining to a first user.

[042] According to a third aspect of the present invention, there is provided a token server for facilitating processing of a financial transaction, operably connected to a network and configured to generate a token, add the token into a blockchain and transmit the token to a first intermediary server, via a messaging bus.

[043] In one embodiment of the invention, the token server is further configured to implement a smart contract and add the smart contract into the blockchain.

[044] According to a fourth aspect of the present invention, there is provided a first intermediary server for facilitating processing of a financial transaction, operably connected to a network and a first document store, and configured to transmit one or more documents pertaining to the financial transaction, to the first document store, generate an enriched data record from the one or more documents and add the enriched data record into a blockchain, request generation of a token corresponding to the financial transaction, to a token server, via a messaging bus and transmit the token to the first document store.

[045] In one embodiment of the invention, the first intermediary server is further configured to send a first financial message comprising the token, to

a second intermediary server, indicative of making a payment to a second user.

[046] In one embodiment of the invention, the first intermediary server is further configured to transmit the token to a first digital device.

[047] In one embodiment of the invention, for generation of the enriched data record, the first intermediary server is configured to extract a plurality of attributes from the one or more documents and combine the plurality of attributes to generate the enriched data record.

[048] In one embodiment of the invention, for generation of the enriched data record, the first intermediary server is configured extract a plurality of attributes from the one or more documents, de-identify the plurality of attributes to obtain a plurality of de-identified attributes and combine the plurality of de-identified attributes to generate the enriched data record.

[049] In one embodiment of the invention, for generation of the enriched data record, the first intermediary server is configured to extract a plurality of attributes from the one or more documents, hash the plurality of attributes to generate a plurality of respective hashes and combine the plurality of hashes to generate the enriched data record.

[050] In one embodiment of the invention, the first intermediary server is further configured to assign a payment risk rating to the token.

[051] In one embodiment of the invention, the first intermediary server is further configured to transmit one or more first requests, each comprising the token, to a second intermediary server, via the messaging bus and

receive one or more first responses from the second intermediary server and transmit the one or more first responses to the first document store.

[052] In one embodiment of the invention, the one or more first responses comprise one or more second regulatory compliance documents pertaining to a second user.

[053] In one embodiment of the invention, the first intermediary server is further configured to hash the one or more first responses to regenerate one or more first response hashes and verify the one or more first response hashes with the blockchain, using the token.

[054] In one embodiment of the invention, the first intermediary server is further configured to encrypt each one of the one or more first requests with a second public key and sign each one of the one or more first requests with a first public key, before transmission to the second intermediary server and decrypt each one of the one or more first responses with a first private key after reception from the second intermediary server.

[055] In one embodiment of the invention, the first intermediary server is further configured to receive the one or more second requests from a second intermediary server and transmit the one or more second requests to the first document store, generate one or more second responses, each comprising the token, corresponding to the respective one or more second requests, transmit the one or more second responses to the second intermediary server, via the messaging bus, hash the one or more second requests and the one or more second responses to generate one or more second request hashes and one or more second response hashes, respectively and add the one or more second request hashes and the one

or more second response hashes to the enriched data record in the blockchain.

[056] In one embodiment of the invention, the first intermediary server is further configured to encrypt each one of the one or more second responses with a second public key and sign the each one of the one or more second responses with a first public key, before transmission to the second intermediary server and decrypt each one of the one or more second requests with a first private key after reception from the second intermediary server.

[057] In one embodiment of the invention, the first intermediary server is further configured to add the first public key into the blockchain.

[058] According to a fifth aspect of the present invention, there is provided a second intermediary server for facilitating processing of a financial transaction, operably connected to a network and a second document store, and configured to receive the token from the second digital device, transmit the token to the second document store and send a second financial message comprising the token to a first intermediary server, indicative of making a payment to a first user.

[059] According to a sixth aspect of the present invention, there is provided a second intermediary server for facilitating processing of a financial transaction, operably connected to a network and a second document store, and configured to receive one or more first requests, each comprising a token, from a first intermediary server and transmit the one or more first requests and the token to the second document store, generate the one or more first responses, each comprising the token, corresponding to the respective one or more first requests, transmit the one or more first

responses to the first intermediary server, via a messaging bus, hash the one or more first requests and the one or more first responses to generate one or more first request hashes and one or more first response hashes, respectively and add the one or more first request hashes and the one or more first response hashes to the enriched data record in the blockchain.

[060] In one embodiment of the invention, the second intermediary server is further configured to encrypt each one of the one or more first responses with a first public key and sign the each one of the one or more first responses with a second public key, before transmission to the first intermediary server and decrypt each one of the one or more first requests with a second private key after reception from the first intermediary server.

[061] According to a seventh aspect of the invention, there is provided a second intermediary server for facilitating processing of a financial transaction, operably connected to a network and a second document store, and configured to transmit one or more second requests, each comprising a token, to a first intermediary server, via a messaging bus and receive one or more second responses from the first intermediary server and transmit the one or more second responses to the second document store.

[062] In one embodiment of the invention, the second intermediary server is further configured to hash the one or more second responses to regenerate one or more second response hashes and verify the one or more second response hashes with the blockchain, using the token.

[063] In one embodiment of the invention, the second intermediary server is further configured to encrypt each one of the one or more second requests with a first public key and sign each one of the one or more second requests with a second public key, before transmission to the first intermediary server

and decrypt each one of the one or more second responses with a second private key after reception from the first intermediary server.

[064] In one embodiment of the invention, the second intermediary server is further configured to add the second public key into the blockchain.

[065] In one embodiment of the invention, the one or more second responses comprise one or more first regulatory compliance documents pertaining to a first user.

[066] Other aspects of the invention are also disclosed.

Brief Description of the Drawings

[067] Notwithstanding any other forms which may fall within the scope of the present invention, a preferred embodiment / preferred embodiments of the invention will now be described, by way of example only, with reference to the accompanying drawings in which:

[068] Fig. 1 illustrates a top level diagram of a system of computing devices to which various embodiments described herein may be implemented;

[069] Fig. 2 illustrates a subsystem of the computing devices for generation of a token, in accordance with a preferred embodiment of the present invention;

[070] Fig. 3 illustrates a subsystem of the computing devices for exchange of requests and responses between two intermediary servers, via a messaging bus, in accordance with a preferred embodiment of the present invention;

[071] Fig. 4 illustrates a subsystem of the computing devices for making a payment to a second user, by a first user, in accordance with a preferred embodiment of the present invention;

[072] Fig. 5 illustrates a subsystem of the computing devices for making a payment to the first user, by the second user, in accordance with a preferred embodiment of the present invention;

[073] Fig. 6 illustrates a computing device to which various embodiments described herein may be implemented; and

[074] Fig. 7 illustrates a computer implemented method for processing a financial transaction, in accordance with a preferred embodiment of the present invention;

[075] Figure 8A is a block diagram of the entities and intermediaries involved in a prior art electronic settlement system;

[076] Figure 8B is a data and funds flow according to a prior art settlement system;

[077] Figure 9A, 9B is a data and funds flow diagram according to an indicative embodiment of the present invention;

[078] Figure 9C is a block diagram of the basic infrastructure and components suited for use with embodiments of the present invention;

[079] Figure 10 A, B, C comprise block diagrams of the steps in a settlement transaction in accordance with a first preferred embodiment of the present invention;

[080] Figure 11 is a block diagram of salient characteristics of a messaging system 810 of the prior art as compared with the salient messaging characteristics of the system 1010 enabled by the code of a second embodiment;

[081] Figure 12 illustrates the options for data content to be included in tokens in accordance with embodiments of the invention as described above;

[082] Figure 13 provides a comparison of characteristics of embodiments of the present invention as compared with the prior art Swift-based messaging system;

[083] Figure 14 is a block diagram in accordance with a further preferred embodiment of the present invention;

[084] Figures 15A and15B are block diagrams of an implementation of a blockchain arrangement suitable for use with the system of embodiments of the invention;

[085] Figure 16 is a block diagram in accordance with yet a further preferred embodiment of the present invention and;

[086] Figure 17 is a detailed block diagram of the system of figure 10C and figure 16;

Description of Embodiments

[087] It should be noted in the following description that like or the same reference numerals in different embodiments denote the same or similar features.

System 100 of computing devices

[088] Fig. 1 shows a system 100 of computing devices adapted for implementation of various embodiments of the present invention.

[089] As such, the system 100 comprises a first digital device 110 and a second digital device 114 connected to a network 116. According to various embodiments, the first digital device 110 is one of, but not limited to, a mobile phone, a desktop computer, a laptop or a tablet etc. Similarly, according to various embodiments, the second digital device is one of, but not limited to, a mobile phone, a desktop computer, a laptop or a tablet etc. Further, the network 116 is one of, but not limited to, a Wide Area Network (WAN) or a Local Area Network (LAN). Preferably the network 116 is internet. The first digital device 110 and the second digital device 114 are also able to communicate through a second network 112. In one embodiment of the invention, the second network 112 is a telecommunication network such as internet or a mobile telecommunication network. In another embodiment, the second network 112 is a non-telecommunication network such as Bluetooth and Near Field Communication (NFC) etc.

[090] Further, the system 100 comprises a first intermediary server 126 and a second intermediary server 128 connected to the network 116. In one embodiment of the invention, the first intermediary server 126 and the second intermediary server 128 represent a first financial institution and a second financial institution, respectively. In one embodiment of the invention, the respective first and second financial institutions are different branches of different of different banks. In another embodiment, the respective first and second financial institutions are different branches of a single bank. In various other embodiments, the respective first and second financial institutions are, but not limited to, commercial banks, investment banks, brokerages, investment companies etc. It is to be noted that each

one of the first intermediary server 126 and the second intermediary server 128 may represent a system of servers comprising web servers, application servers, database servers and gateway servers.

[091] Further, the first intermediary server 126 is operably connected to a first document store 132 and the second intermediary server 128 is operably connected to the second document store 134. In one embodiment, the first document store 132 and the second document store 134 represent databases configured to store a plurality of documents. Each one of the documents comprise data pertaining to a financial transaction and metadata corresponding to the data. In various embodiments, metadata comprises format, encoding, author, hash, verification and relationships to other documents.

[092] Further, the system 100 comprises a financial messaging server 130 connected to the network 116. The financial messaging server 130 provides a financial messaging service between any two intermediary servers, including the first intermediary server 126 and the second intermediary server 128. Some of the examples of financial messaging services include SWIFT (Society for Worldwide Interbank Financial Telecommunication) for cross border transactions. ACH (Automated Clearing House) used in USA and RTGS (Real Time Gross Settlement) used in India and Hong Kong.

[093] Further, the system 100 comprises a token server 120 connected to the network 116 and a token database 122. Further, a blockchain 124 is connected to the network 116. Further, a messaging bus 118 is connected to the network 116. The messaging bus 118 represents a messaging server or a system of messaging servers configured to enable a plurality of applications/servers/devices to communicate with each other. In one embodiment, the messaging bus 118 also comprises an authentication/ authorization server for authorizing the computing devices communicating

through the messaging bus 118. The detailed configuration of the messaging bus 118 has been described in the discussion to follow.

[094] Also, a blockchain 124 is connected to the network 116. The configuration and/or the functioning of the first intermediary server 126, the second intermediary server 128, the first document store 132, the second document store 134, the token server 120, the token database 122, the blockchain 124, and the messaging bus 118 has been described below in a description. The system 100 for processing a financial transaction involves subsystems of the computing devices, which have been depicted by means of figures and description as following. The description below has been explained with embodiments comprising a financial transaction between a first user and a second user. In some embodiments, the first user acts as a biller/ beneficiary/payee and the second user acts as purchaser/payer. In other embodiments, the first user acts as a payer and the second user acts as a payee/beneficiary. Further, it is to be noted that the first user and the second user may represent any number of entities involved in the financial transaction.

[095] In one embodiment of the invention, the first user may instruct the first intermediary sever 126 to process the financial transaction. In one embodiment, the financial transaction involves generation of an invoice for the second user and receiving a payment from the second user, by the first user. In another embodiment, the financial transaction involves making the payment to the second user, by the first user. Specifically, the first user connects with the first intermediary server 126 through the network 116, using the first digital device 110.

[096] Figure 2 illustrates a subsystem (200) of the computing devices for generation of a token, in accordance with a preferred embodiment of the present invention. As shown in figure 2, the first digital device 110

comprises a first processor 210 operably connected to a first memory 220. The first memory 220 comprises a first computer program code, the first computer program code when executed by the first processor 210 instructs the first processor 210 to instruct the first intermediary server 126 to process the financial transaction. Further, in one embodiment of the invention, the first computer program code further instructs the first processor 210 to provide one or more documents pertaining to the financial transaction, to the first intermediary server 126. In another embodiment, the one or more documents are already available with the first intermediary server 126. In yet another embodiment, the first intermediary server 126 is configured to generate at least one document from the one or more documents.

[097] The at least one document may be, but is not limited to, a request for processing the financial transaction. The first intermediary server 126 is configured to transmit the one or more documents pertaining to the financial transaction, to the first document store 132. In one embodiment of the invention, the one or more documents comprise payment metadata such as, but is not limited to, account numbers of the first user (or a beneficiary), Business Identifier Codes (BIC) of the financial institutions corresponding to the first intermediary server 126 and the second intermediary server 128, amount of currency to be transferred and type of currency etc.

[098] Further, in accordance with an embodiment, the one or more documents comprise one or more first regulatory compliance documents pertaining to the first user. Some examples of the regulatory compliance documents include, but are not limited to purpose of payment documents, a result of sanctions screening and secondary identifiers such as date of birth proof, address proof or other Know Your Customer (KYC) documents.

[099] The first intermediary server 126 is further configured to generate an enriched data record from the one or more documents and add the enriched

data record into the blockchain 124. The first intermediary server 126 is configured to generate the enriched data record in multiple ways in multiple embodiments, some of the embodiments have been elucidated below.

[0100] In one embodiment of the invention, the first intermediary server 126 is configured to extract a plurality of attributes from the one or more documents. The plurality of attributes may comprise, but are not limited to, originator attributes, beneficiary attributes and purpose of payment etc. Further, the first intermediary server 126 is configured to combine the plurality of attributes to generate the enriched data record. In another embodiment of the present invention, the first intermediary server 126 is configured to extract the plurality of attributes from one or more documents, de-identify the plurality of attributes to obtain a plurality of de-identified attributes and combine the plurality of de-identified attributes to generate the enriched data record. In yet another embodiment of the present invention, the first intermediary server 126 is configured to extract the plurality of attributes from the one or more documents, hash the plurality of attributes to generate a plurality of respective hashes and combine the plurality of hashes to generate the enriched data record.

[0101] Further, the blockchain 124 is a data structure comprising a plurality of blocks of data. Each block of data from the plurality of blocks of data represents a single financial transaction. Further, the blockchain 124 is configured to store data pertaining to the financial transaction in association with the token. The data pertaining to the financial transaction includes, but is not limited to, the enriched data record, a plurality of hashes, a plurality of public keys etc. Also the blockchain 124 is configured to return the data pertaining to the financial transaction, when queried using the token.

[0102] Further, the first intermediary server 126 is configured to request generation of a token, to the token server 120, via the messaging bus 118.

The token server 120 in turn is configured to generate the token and add the token into the blockchain 124. The token is stored in the blockchain 124, in association with the enriched data record. Further, the token server 120 is configured to transmit the token to the first intermediary server 126, via the messaging bus 118. Further, the first intermediary server 126 is configured to transmit the token to the first document store 132. The token is stored in the first document store 132, in association with the one or more documents.

[0103] In one embodiment of the invention, the token server 120 is further configured to implement a smart contract and add the smart contract into the blockchain 124. In one embodiment, the smart contract is a shared, signed and verifiable program code which is distributed and/or executed on the blockchain 124. The smart contract would run on the blockchain 124 and would be stored in association with the token.

[0104] In one embodiment of the invention, before proceeding any further, the first intermediary server 126 may wish to perform certain "checks", by communicating with the second intermediary server 128, via the messaging bus 118. For enabling communication, the first intermediary server 126 is configured to generate a first asymmetrical pair of a first public key and a first private key. Further, the first intermediary server 126 is configured to add the first public key and a first address of the first intermediary server 126 into the blockchain 124. Similarly, the second intermediary server 128 is configured to generate a second asymmetrical pair of a second public key and a second private key. Further, the second intermediary server 128 is configured to add the second public key and a second address of the second intermediary server 128 into the blockchain 124.

[0105] Fig. 3 illustrates a subsystem (300) of the computing devices for exchange of requests and responses between the first intermediary server

126 and the second intermediary server 128, via the messaging bus118, in accordance with a preferred embodiment of the present invention. During communication with the second intermediary server 128, the first intermediary server 126 is configured to transmit one or more first requests, each comprising the token, to the second intermediary server 128, via the messaging bus 118. Examples of one or more first requests comprise, but are not limited to, KYC check and payment acceptance. In one embodiment of the invention, the the one or more first requests are transmitted on basis of a plurality of predefined criterion. For example, if the first intermediary server 126 is required to make the payment to the second intermediary server 128, the first intermediary server 126 may necessitate KYC check of the second user. The second intermediary server 128 is configured to then receive the one or more first requests from the first intermediary server 126 and transmit the one or more first requests and the token to the second document store 134. In one embodiment of the invention, the one or more first requests are transmitted to the second documents store 134 in form of one or more first request documents.

[0106] Further, the second intermediary server 128 is configured to generate one or more first responses, each comprising the token, corresponding to the respective one or more first requests. In one embodiment of the invention, the one or more first responses are generated in form of one or more first response documents at the second intermediary server 128. Further, the second intermediary server 128 is configured to transmit the one or more first responses to the first intermediary server 126, via the messaging bus 118. As an extension of the example above, the second intermediary server 128 may then send a validation successful response to the first intermediary server 126, via the messaging bus 118. In one embodiment of the invention, the one or more first responses comprise one or more second regulatory compliance documents pertaining to a second user.

[0107] Further, the second intermediary server 128 is configured to hash the one or more first requests and the one or more first responses to generate one or more first request hashes and one or more first response hashes, respectively. Also, the second intermediary server 128 is configured to add the one or more first request hashes and the one or more first response hashes to the enriched data record in the blockchain 124. The first intermediary server 126 is then configured to receive the one or more first responses and transmit the one or more first responses to the first document store 132. In one embodiment of the invention, the first intermediary server 126 is further configured to hash the one or more first responses to regenerate the one or more first response hashes. Further, the first intermediary server 126 is configured to verify the one or more first response hashes with the blockchain 124, using the token. The first intermediary server 126 can ensure that the one or more first responses are same as the ones generated at the second intermediary server 128.

[0108] In one embodiment of the invention, to enable secure transmission, the first intermediary server 126 is configured to encrypt each one of the one or more first requests with the second public key and sign each one of the one or more first requests with the first public key, before transmission to the second intermediary server 128. Consequently, the second intermediary server 128 is configured to decrypt the each one of the one or more first requests with the second private key after reception from the first intermediary server 126. In a similar manner, the second intermediary server 128 is configured to encrypt each one of the one or more first responses with the first public key and sign the each one of the one or more first responses with the second public key, before transmission to the first intermediary server 126. Consequently, the first intermediary server 126 is configured to decrypt each one of the one or more first responses with the first private key after reception from the second intermediary server 128.

[0109] The second intermediary server 128 may also request certain compliance checks. Therefore, the second intermediary server 128 is further configured to transmit one or more second requests, each comprising the token, to the first intermediary server 126, via the messaging bus 118. Examples of the one or more second requests comprise, but are not limited to, sender sanctions screening check. The first intermediary server 126 is in turn configured to receive the one or more second requests and transmit the one or more second requests to the first document store 132. In one embodiment of the invention, the one or more second requests are transmitted to the first document store 132 in form of one or more second request documents. Further the first intermediary server 126 is configured to generate one or more second responses, each comprising the token, corresponding to the respective one or more second requests. In one embodiment of the invention, the one or more second responses are generated in form of one or more second response documents. Further, the first intermediary server 126 is configured to transmit the one or more second responses to the second intermediary server 128, via the messaging bus 118. In one embodiment of the invention, the one or more second responses comprise the one or more first regulatory compliance documents pertaining to the first user.

[0110] Further, the first intermediary server 126 is configured to hash the one or more second requests and the one or more second responses to generate one or more second request hashes and one or more second response hashes, respectively. Further, the first intermediary server 126 is configured to add the one or more second request hashes and the one or more second response hashes to the enriched data record in the blockchain 124. The second intermediary server 128 is in turn configured to receive the one or more second responses and transmit the one or more second responses to the second document store 134. In one embodiment of the

invention, the second intermediary server 128 is further configured to hash the one or more second responses to regenerate the one or more second response hashes and verify the one or more second response hashes with the blockchain 124, using the token. Thus ensuring that the one or more second responses are same as those generated at the first intermediary server 126.

[0111] In one embodiment of the invention, to enable secure communication, the second intermediary server 128 is configured to encrypt each one of the one or more second requests with the first public key and sign each one of the one or more second requests with the second public key, before transmission to the first intermediary server 126. Consequently, the first intermediary server 126 is configured to decrypt the each one of the one or more second requests with the first private key after reception from the second intermediary server 128. In a similar manner, the first intermediary server 126 is configured to encrypt each one of the one or more second responses with the second public key and sign the each one of the one or more second responses with the first public key, before transmission to the second intermediary server 128. Consequently, the second intermediary server 128 is configured to decrypt the each one of the one or more second responses with the second private key after reception from the first intermediary server 126.

[0112] The requests and the responses are transmitted in a secure manner across the messaging bus 118, in form of a plurality of messages. It is to be noted that each one of the plurality of messages comprises a content hash of all its contents to ensure that the contents have not been altered during transmission. The request and/or receipt time of the recipient public key are also attached to the plurality of messages. This ensures only recipient can see message contents & ensures revocability of public keys.

[0113] In one embodiment of the invention, the first intermediary server 128 is further configured to assign a payment risk rating to the token. In one embodiment of the invention, the payment risk rating is assigned to the token at the first intermediary server 126 after completion of the communication with the second intermediary server 128. The payment risk rating provides a pointer to the regulatory and other compliance checks performed by the first intermediary server 126 and the second intermediary server 128. In one embodiment of the invention, the first intermediary server 126 is further configured to add the payment risk rating to the enriched data record in the blockchain 124. Further, the blockchain 124 is configured to return the payment risk rating when queried with the token. The payment risk rating enables better straight through processing by reducing exceptions and false positives.

[0114] The token thus generated may be used to make the payment to the second user by the first user or making the payment to the first user, by the second user. Figure 4 illustrates a subsystem (400) of the computing devices for making the payment to the second user, by the first user. As shown in the figure 4, the first intermediary server 126 is configured to send a first financial message comprising the token, to the second intermediary server 128, indicative of making the payment to the second user. The first financial message is sent through the financial messaging server 130.

[0115] Figure 5 illustrates a subsystem (500) of computing devices for making the payment to the first user, by the second user. As shown in the figure 5, the first intermediary server 126 is further configured to transmit the token to the first digital device 110. In turn, the first computer program code instructs the first processor 210 to receive the token from the first intermediary server 126. In one embodiment of the invention, the first processor 210 is further instructed to provide the token to the second digital device 114 via the network 116 or the second network 112. The second

digital device 110 comprises a second memory 520 and a second processor 510 operably connected to the second memory 520, the second memory 520 comprising a second computer program code, the second computer program code when executed by the second processor 510, instructs the second processor 510 to receive the token from the first digital device 110 and provide the token to the second intermediary server 128.

[0116] In turn the second intermediary server 128 is configured to receive the token from the second digital device 114, transmit the token to the second document store 134 and send a second financial message comprising the token, to the first intermediary server 126, indicative of making the payment to the first user. Further, the second financial message is sent through the financial messaging server 130.

Computing device

[0117] Fig. 56 shows a computing device 600. In a preferred embodiment, the computing device 600 takes the form of the first intermediary server 126, the second intermediary server 128, the token server 120 and the financial messaging server 190 as described above. In this manner, the computing device 500 is adapted to comprise functionality for communication with the network 116, storage capability (such as the token database 122) for storing a plurality of tokens and respective creators of the plurality of tokens.

[0118] However, it should be noted that each one first digital device 110 and the second digital device 114, as shown in figure 1, may also be depicted as the computing device 600. In this manner, the computing device may comprise differing technical integers, such as the display device 6020, one or more human interface devices 660 and the like. In other words, the technical integers of the computing device 500 is shown in figure 5 are exemplary only and variations, adaptations and the like may be made

thereto within the purposive scope of the embodiments described herein and having regard for the particular application of the computing device 600.

[0119] In particular the steps of the computer implemented method for processing of a financial transaction, as described in further detail below, may be implemented as computer program code instructions executable by the computing device 600. The computer program code instructions may be divided into one or more computer program code instruction libraries, such as dynamic link libraries (DLL), wherein each of the libraries performs a one or more steps of the computer implemented method. Additionally, a subset of the one or more of the libraries may perform graphical user interface tasks relating to the steps of the computer implemented method.

[0120] The device 600 comprises semiconductor memory 610 comprising volatile memory such as random access memory (RAM) or read only memory (ROM). The memory 600 may comprise either RAM or ROM or a combination of RAM and ROM.

[0121] The device 600 comprises a computer program code storage medium reader 630 for reading the computer program code instructions from computer program code storage media 620. The storage media 620 may be optical media such as CD-ROM disks, magnetic media such as floppy disks and tape cassettes or flash media such as USB memory sticks.

[0122] The device further comprises I/O interface 640 for communicating with one or more peripheral devices. The I/O interface 640 may offer both serial and parallel interface connectivity. For example, the I/O interface 640 may comprise a Small Computer System Interface (SCSI), Universal Serial Bus (USB) or similar I/O interface for interfacing with the storage medium reader 630. The I/O interface 640 may also communicate with the one or more human interface devices (HID) 660 such as keyboards, pointing devices,

joysticks and the like. The I/O interface 640 may also comprise a computer to computer interface, such as a Recommended Standard 232 (RS-232) interface, for interfacing the device 600 with one or more personal computer (PC) devices 690. The I/O interface 640 may also comprise an audio interface for communicate audio signals to one or more audio devices 6050, such as a speaker or a buzzer.

[0123] The device 600 also comprises a network interface 650 for communicating with one or more computer networks 680. The network 680 may be a wired network, such as a wired Ethernet™ network or a wireless network, such as a Bluetooth™ network or IEEE 802.11 network. The network 680 may be a local area network (LAN), such as a home or office computer network, or a wide area network (WAN), such as the Internet or private WAN.

[0124] The device 600 comprises an arithmetic logic unit or processor 6000 for performing the computer program code instructions. The processor 6000 may be a reduced instruction set computer (RISC) or complex instruction set computer (CISC) processor or the like. The device 600 further comprises a storage device 6030, such as a magnetic disk hard drive or a solid state disk drive.

[0125] Computer program code instructions may be loaded into the storage device 6030 from the storage media 620 using the storage medium reader 630 or from the network 680 using network interface 650. During the bootstrap phase, an operating system and one or more software applications are loaded from the storage device 6030 into the memory 610. During the fetch-decode-execute cycle, the processor 6000 fetches computer program code instructions from memory 610, decodes the instructions into machine code, executes the instructions and stores one or more intermediate results in memory 600.

[0126] In this manner, the instructions stored in the memory 610, when retrieved and executed by the processor 6000, may configure the computing device 600 as a special-purpose machine that may perform the functions described herein.

[0127] The device 600 also comprises a video interface 6010 for conveying video signals to a display device 6020, such as a liquid crystal display (LCD), cathode-ray tube (CRT) or similar display device.

[0128] The device 600 also comprises a communication bus subsystem 665 for interconnecting the various devices described above. The bus subsystem 665 may offer parallel connectivity such as Industry Standard Architecture (ISA), conventional Peripheral Component Interconnect (PCI) and the like or serial connectivity such as PCI Express (PCIe), Serial Advanced Technology Attachment (Serial ATA) and the like.

Embodiments of the method

[0129] Figure 7 illustrates a computer implemented method 700 for processing a financial transaction in accordance with an embodiment of the present invention. As described above, the financial transaction is assumed to be taking place between the first user and the second user. The method begins at step 710 by transmitting the one or more documents pertaining to the financial transaction, from the first intermediary server 126 to the first document store 132. In one embodiment of the invention, the one or more documents are provided to the first intermediary server 126 by the first user, from the first digital device 110. In another embodiment, the one or more documents are already available with the first intermediary server 126. In yet another embodiment, the at least one document from the one or more documents is generated at the first intermediary server 126.

[0130] At step 720, the enriched data record is generated from the one or more documents, at the first intermediary server 126. Further, the enriched data record is added into the blockchain 124, from the first intermediary server 126. The enriched data record may be generated in different manners in different embodiments. Some of the embodiments have been discussed below.

[0131] In one embodiment of the invention, the plurality of attributes are extracted from the one or more documents, at the first intermediary server 126. Further, the plurality of attributes are combined to generate the enriched data record at the first intermediary server 126.

[0132] In another embodiment, the plurality of attributes are extracted from the one or more documents, at the first intermediary server 126. Further, the plurality of attributes are de-identified to obtain the plurality of de-identified attributes at the first intermediary server 126. The de-identification of the plurality of attributes comprises removal of any information from the plurality of attributes which may link the plurality of attributes to the first user or the second user. This is to ensure the confidentiality of the first user and the second user, in case the enriched data record is accessed through illegal routes. The plurality of de-identified attributes are then combined, at the first intermediary server 126, to generate the enriched data record.

[0133] In yet another embodiment, the plurality of attributes are extracted from the one or more documents, at the first intermediary server 126. Further, the plurality of attributes are hashed to generate the plurality of respective hashes, at the first intermediary server 126. The plurality of hashes are then combined to generate the enriched data record, at the first intermediary server 126.

[0134] At step 730, the token server 120 is requested to generate the token corresponding to the financial transaction, from the first intermediary server 126, via the messaging bus 118. At step 740, the token is generated at the token server 120. Further, the token is added into the blockchain 124, from the token server 120. At step 750, the token is transmitted from the token server 120 to the first intermediary server 126. At step 760, the token is transmitted from the first intermediary server 126 to the first document store 132. Further, the token is stored in association with the one or more documents, in the first document store 132.

[0135] In one embodiment of the invention, the smart contract is implemented at the token server 120. Further, the smart contract is added into the blockchain, from the token server 120.

[0136] In one embodiment of the invention, the first intermediary server 126 communicates with the second intermediary server 128, via the messaging bus 118. The communication may take place for verification and validation of the first user and the second user. In one embodiment of the invention, the first asymmetrical pair of the first public key and the first private key is generated at the first intermediary server 126. Further, the first public key and the first address of the first intermediary server 126 are added into the blockchain 124, from the first intermediary server 126. Similarly, the second asymmetrical pair of the second public key and the second private key is generated at the second intermediary server. Further, the second public key and the second address of the second intermediary server 128 are added into the blockchain 124, from the second intermediary server 128.

[0137] In one embodiment, during communication, the one or more first requests, each comprising the token, are transmitted from the first intermediary server 126 to the second intermediary server 128, via the messaging bus 118. Further, the one or more first requests are received at

the second intermediary server 128 and the one or more first requests and the token are transmitted from the second intermediary server 128 to a second document store 134. Further, one or more first responses, each comprising the token, corresponding to the respective one or more first requests, are generated at the second intermediary server 128. Further, the one or more first responses are transmitted from the second intermediary server 128 to the first intermediary server 126, via the messaging bus 118. Further, the one or more first requests and the one or more first responses are hashed at the second intermediary server 128 to generate one or more first request hashes and one or more first response hashes, respectively. Further, the one or more first request hashes and the one or more first response hashes are added to the enriched data record in the blockchain 124, from the second intermediary server 128. Also, the one or more first responses are received at the first intermediary server 126 and transmitted to the first document store 132.

[0138] In one embodiment of the invention, the one or more first responses comprise the one or more second regulatory compliance documents pertaining to the second user. Further, in one embodiment of the invention, the one or more first responses are hashed at the first intermediary server 126 to regenerate the one or more first response hashes. Also, the one or more first response hashes are verified with the blockchain 124 from the first intermediary server 126, using the token.

[0139] In one embodiment of the invention, for secure communication, each one of the one or more first requests are encrypted with the second public key and signed with the first public key at the first intermediary server 126, before transmission to the second intermediary server 128. Consequently, the each one of the one or more first requests are decrypted with the second private key at the second intermediary server 128 after reception from the first intermediary server 126. Similarly, each one of the one or more first

responses are encrypted with the first public key and signed with the second public key at the second intermediary server 128, before transmission to the first intermediary server 126. Also, consequently, the each one of the one or more first responses are decrypted with the first private key at the first intermediary server 126 after reception from the second intermediary server 128.

[0140] Similarly, in the present and various other embodiments, during communication, the one or more second requests, each comprising the token, are transmitted from the second intermediary server 128 to the first intermediary server 126, via the messaging bus 118. Further, the one or more second requests are received at the first intermediary server 126 and the one or more second requests are transmitted from the first intermediary server 126 to the first document store 132. Further, one or more second responses, each comprising the token, corresponding to the respective one or more second requests, are generated at the first intermediary server 126. Further, the one or more second responses are transmitted from the first intermediary server 126 to the second intermediary server 128, via the messaging bus 118. Further, the one or more second requests and the one or more second responses are hashed at the first intermediary server 126 to generate one or more second request hashes and one or more second response hashes, respectively. Further, the one or more second request hashes and the one or more second response hashes are added to the enriched data record in the blockchain 124, from the first intermediary server 126. Also, the one or more second responses are received at the second intermediary server 128 and transmitted to the second document store 134.

[0141] In one embodiment of the invention, the one or more second responses comprise the one or more first regulatory compliance documents pertaining to the first user. Further, in one embodiment, the one or more second

responses are hashed at the second intermediary server 128 to regenerate the one or more second response hashes. Also, the one or more second response hashes are verified with the blockchain 124 from the second intermediary server 128, using the token.

[0142] In one embodiment of the invention, for secure communication, each one of the one or more second requests are encrypted with the first public key and signed with the second public key at the second intermediary server 128, before transmission to the first intermediary server 126. Consequently, the each one of the one or more second requests are decrypted with the first private key at the first intermediary server 126 after reception from the second intermediary server 128. Similarly, each one of the one or more second responses are encrypted with the second public key and signed with the first public key at the first intermediary server 126, before transmission to the second intermediary server 128, and decrypted with the second private key at the second intermediary server 128 after reception from the first intermediary server 126.

[0143] In one embodiment of the invention, the payment risk rating is assigned to the token, at the first intermediary server 126. Further, the payment risk rating is added to the enriched data record in the blockchain 124, from the first intermediary server 126.

[0144] In one embodiment, for making the payment to second user, by the first user, the first financial message comprising the token, is sent from the first intermediary server 126 to the second intermediary server 128, indicative of making the payment to the second user. Further, the first financial message is sent via the financial messaging server 130.

[0145] In another embodiment, the token is transmitted from the first intermediary server 126 to the first digital device 110, available with the first

user. The first processor 210 receives the token from the first intermediary server 126 and stores the token in the first memory 220. Further, the token is provided to the second user, by the first user. In one embodiment, the token is provided to the second user by means of a Quick Response (QR) code printed on an invoice. In another embodiment, the token is provided to the second user at the second digital device 114 available with the second user, from the first digital device 110. The second processor 510 receives the token from the first digital device 110, and stores the token in the second memory 520.

[0146] Further, the token is provided to the second intermediary server 128, from the second digital device 114, by the second user. The second computer program code instructs the second processor 510 to provide the token to the second intermediary server. The token is then transmitted to the second document store 134, from the second intermediary server 128. Further, the second financial message is sent from the second intermediary server 128, to the first intermediary server 126, indicative of making the payment to the first user.

Prior Art

[0147] With reference to Figure 8A there is illustrated in block form the basic components of a prior art settlement system. In many transactions there will be an at least first transacting entity 811 which enters into a financial transaction with an at least second transacting entity 812. The financial transaction may be as simple as the agreement by the first transacting entity 811 to sell a particular item or service to the second transacting entity 812. Typically the financial transaction will require settlement for an agreed amount expressed in a Fiat or other currency. In the vast majority of cases the at least first transacting entity 811 will be associated with an at least first

intermediary entity 813, in this instance in the form of a bank A and similarly the second transacting entity 812 will be associated with an at least second intermediary entity 814 in this instance in the form of bank B. The first transacting entity 811 will have a first bank account 815 at the first intermediary entity 813 whilst second transacting entity 812 will have a second bank account 816 at second intermediary entity 814. Settlement of any given transaction requires instruction given by first transacting entity 811 to its first intermediary entity 813 to pay an agreed amount from the first bank account 815 to the bank account comprising second bank account 816 of second intermediary entity 814 of second transacting entity 812. For these instructions to be carried out metadata in the form of payment metadata 817 must be assembled at the first intermediary entity 813 sufficient and exhaustive to communicate to the second intermediary entity 814 such that the agreed settlement amount is transmitted from bank A to bank B and more particularly to the specific accounts of the respective first transacting entity 811 and second transacting entity 812.

[0148] A similar transaction may be applied in reverse where the second transacting entity sells a good or service to first transacting entity 811. In such an instance the respective intermediaries, once having received the respective payment metadata 817 and exchanged that metadata 817 may elect to simply pay the difference 818 electronically as between the intermediaries to effect the multiple transactions. In some instances, particularly where the financial transaction is cross-border-for example the first intermediary entity 813 is in a first country whilst the second intermediary entity 814 is in a second country the metadata 817 may include what is known as a Swift code which is a substantially unique identifier for each intermediary entity involved in the financial transaction. However, for any given transaction, far more data than merely a unique identifier for each intermediary entity involved in a financial transaction is required in order for

the appropriate settlement amounts to ultimately be recorded in the correct accounts and settle the financial transaction for the agreed amounts.

[0149] Figure 8B is a data and funds flow diagram of data and funds flow according to a prior art settlement system at the granular level. In this instance, with reference to figure 8B like components are numbered as for figure 8A a given transaction requiring settlement can be embodied as a bill 890 which will include payment data 891 and may include bank facilitation payment data 892 comprising, in this instance, a biller code and a financial transaction code. Banks which are party to this bank facilitation payment system permit data entry by entity B (or payer B) 812 into a database of bank B 814 by means of a bank application or web interface 814 B. Bank B may then add additional data to form metadata 817 which is sent to a third-party server 893 which utilises metadata 817 to trigger pay (settlement) of bill 890 from payer B bank 814 to biller A bank 813.

Exemplary Embodiments

[0150] With reference to Figure 9C there is illustrated a block diagram of the basic infrastructure and components suited for use with embodiments of the present invention. In this instance like components are numbered as for figure 8 except in the 900 series. So, for example, first transacting entity 811 becomes first transacting entity 911 in this embodiment with reference to figure 2C.

[0151] In this instance a settlement system 910 according to a generalised embodiment includes at least first transacting entity 911 which enters into a financial transaction with at least a second transacting entity 912. As previously these entities are associated with a respective first intermediary entity 913 and a second intermediary entity 914 in the form of bank A and

bank B. Each of the first transacting entity 911 and a second transacting entity 912 has a respective account 915, 916 at their respective intermediary entities as illustrated in figure 9C

[0152] In this instance, in the event that first transacting entity 911 enters into a financial transaction with second transacting entity 912 then, at the time of entry into the financial transaction 920, a token 921 is generated. In this instance the token 921 is generated by at least first digital device 922 communicating with a token database 923. The token database 923 generates a token comprising a data file 924 containing all data that will ultimately be required to settle the financial transaction 920 including any necessary identifying information for the transacting entity is, their accounts and the intermediary entities. Settlement is effected by communication of the token 921 to bank A and then to bank B together with the appropriate flow of funds.

[0153] With reference to figure 9A at the granular level a bill 990 from a biller 911 directed to a payer 912 contains bill data 991 and also token data of a token 921 residing within a code symbol 994 (in this instance a QR code). The token data includes pointer data pointing to data 995 on token database 923. The data 995 combined with bank ID data 914 permits the creation by token database 923 of a full payment record 996 which can be utilised to cause settlement of the bill 990 as against payer 912 via, in this instance, their respective banks 914, 913.

[0154] With reference to figure 9B the payment data record 996 is utilised has fed into a settlement network such as, for example a network 997 operating under the Ripple protocol thereby permitting substantially real-time settlement across multiple institutions and banks.

[0155] With reference to Figures 10 there is illustrated in block diagram form a first preferred embodiment of the present invention by way of a non-limiting example of a financial transaction. In this embodiment like components are numbered as for the previous embodiments except in the 1000 series. So, for example, token 921 becomes token 1021.

[0156] With reference to figure 10A the financial transaction system 1010 is activated, as for the previous embodiment, when a financial transaction 1020 is entered into between at least first transacting entity 1011 and at least a second transacting entity 1012 each dealing, for the purposes of this transaction, through respective intermediary entities 1013, 1014.

[0157] At the time of and as part of entry into the financial transaction 1020 the first transacting entity 1011 accesses token database 1023 via digital device 1022 executing via a web browser interface or via execution of an application running on a portable digital devices such as a mobile telephone or in a further alternative as a point-of-sale terminal in order to arrange for the database 1023 to generate a token 1021. In this instance the token 1021 will include better data 1024 including the recipient named, BIC, IBAN, destination country, mobile number, currency, business type, communication, payment amount. In this instance the token 1021 including the metadata 1024 is stored in the token database 1023. In addition the first transacting entity 1011 communicates the token 1021 to a digital device 1030 associated with second transacting entity 1012. In this instance the communication is by way of initial transmission of the token 1021 to digital device 1022 which then on transmits the token via Internet 1031 to digital device 1030.

[0158] With reference to figure 10B, when ready to settle the financial transaction 1020 the second transacting entity 1012 "logs in" to a portal associated with second intermediary entity 1014 and communicates the

token 1021. In this instance have the login can be executed via a web browser associated with digital device 1030 which communicates via Internet 1031 the token 1021 to a digital processing system 1032 (including at least a processor and a memory) associated with second intermediary entity 1014. Substantially at the same time as part of seeking to settle the financial transaction 1020:

[0159] Notification: token database 1023 notifies second intermediary entity 1014 to contact the token database 1023 from which it receives a further token 1021A.

[0160] Verification: token database 1023 communicates with the processing system 1032 of second intermediary entity 1014 to verify that sufficient funds are located in account 1016 as indicated in the meta data 1024 to settle the financial transaction.

[0161] Committing payer funds: payers bank debits payers account: payers bank sends notice to payer bank gateway: payers bank gateway calls token database 1023 to get approved token:

[0162] Settlement: gateway of payers bank sends by way of non-limiting example XRP (the native currency of the Ripple protocol) to billers bank gateway: payers bank gateway notifies token database 1023 of receipt:

[0163] Clearing: payer's bank Nostro account is debited subject to bank institution rules.

[0164] Examples of tokenised messages and their generation and transmission are illustrated in pseudocode at the end of the description before the claims. Reference to "sparro" is a reference to an instance of a token databasep23.

[0165] features of this embodiment include the enablement of a private, invitation only, network for banking institutions which, in a particular form, can facilitate cross-border payments thereby to enable substantially real-time payments at reduced processing cost.

[0166] With reference to figure 11 there is shown a block diagram of salient characteristics of a messaging system 810 of the prior art as compared with the salient messaging characteristics of the system 1010 enabled by the code listed above and more broadly described with reference to the earlier embodiments.

[0167] Figure 12 illustrates the options for data content to be included in tokens in accordance with embodiments of the invention as described above.

[0168] Figure 13 provides a comparison of characteristics of embodiments of the present invention as compared with the prior art Swift-based messaging system at a commercial layer 1270, a security layer 1271 and a technical layer 1272

[0169] Embodiments of the invention can be implemented utilising the "Ripple" the framework, protocol and gateway-or more generally any blockchain based framework. In a particular form the final settlement process can be enabled through a Ripple frame work thereby to facilitate substantially real-time settlement across multiple institutions and multiple banks.

[0170] Figure 14 is a block diagram of a further embodiment. In this instance a distributed ledger 1381 operating on blockchain principles provides for transmission of the tokenised message as for previous embodiments.

[0171] In this instance it will be observed that the tokenised transmission distributed ledger 1381 operates in parallel with conventional transmission between institution A and institution B.

[0172] Conventional transmission includes transmission of conventional messages utilising the SWIFT protocol. It is also to be noted that institution A and institution B may be subsidiaries of the same institution or may otherwise be closely related. In the alternative they may be completely independent institutions.

[0173] The tokenised message as described in previous embodiments may include information as typically transmitted by the SWIFT or other current acknowledged data transmission systems for transmission of financial information for the purpose of transfer of funds between parties.

[0174] The tokenised message may transmit data which includes some of the data normally included in the conventional message. In alternative forms it may include additional data. In yet alternative forms it may include data not transferred at all in the data normally included in the conventional message.

[0175] The aim, in particular forms, ultimately, is to improve the reliability of the financial transaction as between the first transacting entity and the second transacting entity and, in some forms, to provide an enhanced capability.

[0176] In the arrangement of figure 14 the data comprising the tokenised message is transmitted via nodes 1380 within a blockchain 1381.

[0177] In summary, Bank A and Bank B might be branches of the same bank, say HSBC HK and HSBC China (which today use SWIFT for intrabank transfers). So this system could be used within 1 financial institution.

[0178] In one form the purpose of storing the token only in the blockchain is really to both de-identify the information in the blockchain (which is critical for banks), and enable use of existing (SWIFT / ACH / RTGS) or new messaging systems to send the payment instruction in tokenised format. Banks today have significant investment in existing conventional messaging systems and a complete abandonment of these messaging systems would not be feasible. However settlement is still a manual process so linking the conventional messaging system to the 'blockchain' settlement system (via the token) is an important feature of this embodiment. So, in diagram 7 we include a SWIFT/ACH/RTGS connection between the two Financial Institutions (FIs) (or branches) for communication of the token, and the blockchain ledger is common. The data that is required to settle the payment can be provided by the FI's customer or by the FI themselves (say from a core banking system or similar).

[0179] Fig 15 illustrates in block diagram form key components of an implementation of a blockchain structure which may be utilised to implement the system of figure 14.

[0180] Each block includes verified transactions and the blockchain maintains a ledger all prior transactions. The blockchain is duplicated by all the computers on a network.

[0181] The first block in the chain is known as the Genesis block and new blocks can be added in linear and chronological order. From any given block in the chain the information of this genesis block and all blocks that led back to this one can be retrieved. A blockchain is essentially numerous blocks connected through hash chaining where each block is comprised of the following (see figure 15);

[0182] Timestamp: provides proof that the data in a block existed at a particular time;

[0183] Previous Hash: Essentially a pointer to the previous block;

[0184] Merkle Hash: Summary of all executed transactions;

[0185] Nonce: Individual blocks identity and is an arbitrary number which can only be used once.

[0186] The blockchain is managed by a network of distributed nodes where each node contains a copy of the entire blockchain. Each node in the network can add blocks to the chain, where every node is adding blocks at the same point in the chain at the same time. The more nodes that comprise the network the harder it is to disrupt the storage of the blockchain. Unlike centralised systems which rely on a single authority, there is no single point of failure in these distributed nodes network. If you change the content of a block you change its Hash.

[0187] Blockchains can be based on/ operate in association with any one of a number of protocols – for example Ripple or Stellar.

[0188] Figure 15B shows a first step in creation of records in the block chain structure of figure 15A whilst figure 15C shows a second step in the creation of records in the chain structure of figure 15A. The chain structures of this type may be utilised in relation to the embodiments described in this application.

[0189] Figure 16 is a block diagram of a further embodiment wherein the parallel data transmission capabilities of the system are further detailed as compared with the embodiment of figure 14 .Components are numbered as for previous embodiments except in the 1400 series. So, for example, first transacting entity 1311 of the further embodiment of figure 14 becomes the first transacting entity 1411. In this instance a distributed ledger 1481

operating on blockchain principles (refer description with reference to figure 15) provides for transmission of the tokenised message as for previous embodiments.

[0190] In this instance it will be observed that the tokenised transmission distributed ledger 1481 operates in parallel with conventional transmission between institution A and institution B.

[0191] Conventional transmission includes transmission of conventional messages utilising the SWIFT protocol. It is also to be noted that institution A 1413 and institution B 1414 may be subsidiaries of the same institution or may otherwise be closely related. In the alternative they may be completely independent institutions.

[0192] The tokenised message 1490 as described in previous embodiments may include information as typically transmitted by the SWIFT or other current acknowledged data transmission systems for transmission of financial information for the purpose of transfer of funds between parties.

[0193] The tokenised message may transmit data which includes some of the data normally included in the conventional message. In alternative forms and more particularly the form with reference to figure 16 it may include additional data however, in this instance the additional data 1491 is transmitted via blockchain 881 as an entry in a shared ledger 1492. The additional data 1491 in this instance comprises a token value 1493, a financial transaction value 1494 a sender cheque status flag 895 and a token state 1496. This entry 1497 in shared ledger 1492 can be accessed based on token value 1493. In an alternative form the entry 1497 and more particularly the token value 1493 may be secured for example requiring a separate key before the data can be accessed and/or decrypted. The data in entry 1497 may comprise deidentified data thereby to ensure that no

personally identifiable information is transmitted to Bank (second intermediary entity 1414).

[0194] The aim, ultimately, is to improve the reliability of the financial transaction as between the first transacting entity and the second transacting entity and, in some forms, to provide an enhanced capability.

[0195] In particular, in preferred forms an element includes provision of systems which add additional information whereby the additional information is to enrich payments with more information given the inability of existing payment systems to communicate enriched information.

[0196] In the arrangement of figure 16 the data comprising the tokenised message is transmitted via nodes 1480 within a blockchain 1481.

[0197] In summary, Bank A and Bank B might be branches of the same bank, say HSBC HK and HSBC China (which today use SWIFT for intrabank transfers). So this system could be used within 1 financial institution.

[0198] In one form the purpose of storing the token only in the blockchain is really to both de-identify the information in the blockchain (which is critical for banks), and enable use of existing (SWIFT / ACH / RTGS) or new messaging systems to send the payment instruction in tokenised format. Banks today have significant investment in existing conventional messaging systems and a complete abandonment of these messaging systems would not be feasible. However settlement is still a manual process so linking the conventional messaging system to the 'blockchain' settlement system (via the token) is an important feature of this embodiment. So, in figure 16 we include a SWIFT/ACH/RTGS connection between the two Financial Institutions (FIs) (or branches) for communication of the token, and the blockchain ledger is common. The data that is required to settle the

payment can be provided by the FI's customer or by the FI themselves (say from a core banking system or similar).

[0199] Figure 17 is a detailed block diagram of the system of figure 10C and figure 16.

[0200] With reference to Figure 17 there is illustrated in block diagram form a first preferred embodiment of the present invention by way of a non-limiting example of a financial transaction. In this embodiment like components are numbered as for Figure 16 in the 1400 series.

[0201] With reference to figure 17 the financial transaction system 1010 is activated, as for the previous embodiment, when a financial transaction 1020 is entered into between at least first transacting entity 1011 and at least a second transacting entity 1012 each dealing, for the purposes of this transaction, through respective intermediary entities 1013, 1014.

[0202] At the time of and as part of entry into the financial transaction 1020 the first transacting entity 1011 accesses token database 1023 via digital device 1022 executing via a web browser interface or via execution of an application running on a portable digital devices such as a mobile telephone or in a further alternative as a point-of-sale terminal in order to arrange for the database 1023 to generate a token 1021. In this instance the token 1021 will include better data 1024 including the recipient named, BIC, IBAN, destination country, mobile number, currency, business type, communication, payment amount. In this instance the token 1021 including the metadata 1024 is stored in the token database 1023. In addition the first transacting entity 1011 communicates the token 1021 to a digital device 1030 associated with second transacting entity 1012. In this instance the communication is by way of initial transmission of the token 1021 to digital

device 1022 which then on transmits the token via Internet 1031 to digital device 1030.

[0203] With reference to figure 17, when ready to settle the financial transaction 1020 the second transacting entity 1012 "logs in" to a portal associated with second intermediary entity 1014 and communicates the token 1021. In this instance have the login can be executed via a web browser associated with digital device 1030 which communicates via Internet 1031 the token 1021 to a digital processing system 1032 (including at least a processor and a memory) associated with second intermediary entity 1014. Substantially at the same time as part of seeking to settle the financial transaction 1020:

[0204] Notification: token database 1023 notifies second intermediary entity 1014 to contact the token database 1023 from which it receives a further token 1021A.

[0205] Verification: token database 1023 communicates with the processing system 1032 of second intermediary entity 1014 to verify that sufficient funds are located in account 1016 as indicated in the meta data 1024 to settle the financial transaction.

[0206] Committing payer funds: payers bank debits payers account: payers bank sends notice to payer bank gateway: payers bank gateway calls token database 1023 to get approved token:

[0207] Settlement: gateway of payers bank sends by way of non-limiting example XRP (the native currency of the Ripple protocol) to billers bank gateway: payers bank gateway notifies token database 1023 of receipt:

[0208] Clearing: payer's bank may be a Nostro account which is debited subject to bank institution rules.

[0209] Embodiments of the invention can be implemented utilising the "Ripple" framework, protocol and gateway-or more generally any blockchain based framework. In a particular form the final settlement process can be enabled through a Ripple framework thereby to facilitate substantially real-time settlement across multiple institutions and multiple banks.

[0210] With further reference to figure 17 it will be observed that the token 1021, in this instance, may be conveyed between bank 1013 and bank 1014 by way of a medium 1060 utilizing the SWIFT protocol or other compatible protocols 1050. In preferred forms the medium the medium will be an electronic communications medium and in particular forms may be implemented by way of a VPN established between bank 1013 and bank 1014.

[0211] Separately deidentified data 1051 A, B, C, D associated with the financial transaction to which the token pertains may be transmitted over a separate communication medium, in this instance internet 1031. In a preferred form the communication medium utilizes a blockchain structure as described earlier in this specification and the deidentified data 1051 A, B, C, D is located within a record structure 1061 which is replicated throughout the blockchain structure.

[0212] In use a sellers bank 1013 as part of entering into the financial transaction with buyers bank 1014 will establish a SWIFT transaction transmittable over medium 1060. Separately and preferably in parallel the sellers bank 1013 will perform associated operations needed to complete the financial transaction such as verification of the buyers ID and related characteristics. Data related to these associated operations is then placed

in record structure 1061 and that record is placed into the blockchain structure. The associated data includes deidentifed data 1051 A, B, C, D.

[0213] This data is available to the buyers bank 1014 by way of the buyers bank logging into the blockchain structure and receiving the deidentified data which is associated with the financial transaction which is represented by token 1021. Thereby allowing assembly by the buyers bank 1014 of all necessary data to execute the financial transaction on behalf of the buyer and seller.

[0214] With reference to figures 16 and 17 the system provides for communication of invoice/purchase order /remittance advice information as illustrated.

[0215] It will be further observed that blockchain structures may be utilized to provide an information layer above existing legacy systems (for example based on SWIFT protocols and the like) and wherein the additional information layer provides enriched information about payments using the token. It is to be noted that existing systems do not provide enriched information and, in more particular forms, do not provide deidentified information/data for use by the communicating parties.

[0216] The above describes only some embodiments of the present invention and modifications, obvious to those skilled in the art, can be made thereto without departing from the scope of the present invention.

[0217] The computer implemented method and the system for processing a financial transaction offers a plurality of advantages. First, the invention enables a wide variety of documents to be attached to a financial transaction, by means of a token. The existing financial messaging systems allow only specific information to be attached to the financial transaction.

Further, the invention enables generation of an auditable enriched data record from the documents. The enriched data record is stored in a distributed ledger (or the blockchain) and can be retrieved at any time when queried with the token. Further, the enriched data record ensures that integrity of the documents is maintained in perpetuity. Further, the documents stores enable maintaining of a state of the token. That is, a status of the financial transaction can be tracked at any time, from the respective documents stored in the document stores.

Other Exemplary Embodiments

[0218] Definitions:

[0219] Token: in this specification a "token" is a pointer to an enriched data record of a plurality data required to process a financial transaction and wherein the plurality of data is rendered, formatted or passed through an algorithm in a predetermined manner. The process of rendering, formatting or passing through an algorithm in a predetermined manner is termed “tokenisation”. The tokenisation process may involve operations such as encryption and de-identification of the plurality of data.

[0220] Financial Transaction: in this specification "financial transaction" refers to a trade between two parties, for example at least a first transacting entity and a second transacting entity and wherein the trade is expressed in a financial form (for example in a Fiat currency or an electronic currency-to be distinguished, for example, from a barter transaction) which will ultimately require exchange of currency to process the financial transaction. In some instances the currency will be the same on both sides of the financial transaction. In other cases a conversion from one currency to another may be required.

[0221] Personally Identifiable Information (PII): in this specification refers to information that a regulator or privacy policy will not allow to be disclosed to a third party.

[0222] Accordingly, in one broad form of the invention, there is provided a system for settling a financial transaction electronically; said system comprising:

at least a first transacting entity;

at least a second transacting entity;

at least a first intermediary entity;

at least a second intermediary entity;

in the case where the first transacting entity enters into a financial transaction with the second transacting entity generating a tokenised message at the time of the financial transaction containing data needed to settle the financial transaction;

initiating settlement of the financial transaction by transmission of the tokenised message to the at least first transacting entity.

[0223] In a further broad form of the invention there is provided a tokenised message construction system; said system comprising:

a server in communication with a database and which facilitates communications between a plurality of parties to a financial transaction;

each party having a digitised device with which to communicate with other ones of the parties and with the server;

each party capable of generating a tokenised message via a bidirectional communication with the server.

[0224] Accordingly, in yet a further broad form of the invention there is provided tokenised message construction system; said system comprising:

a server in communication with a database and which facilitates communications between a plurality of parties to a financial transaction;

each party having a digitised device with which to communicate with other ones the parties and with the server;

each party capable of generating a tokenised message via a bidirectional communication with the server.

[0225] Preferably the tokenised message is generated with reference to a token database located at a remote location.

[0226] Preferably the tokenised message includes at least a first data element, a second data element and a third data element.

[0227] Preferably the first data element comprises identification data for a payor, the second data element comprises identification data for a payee (biller) and the third data element comprises identification currency, denomination and value data.

[0228] Preferably a further tokenised message is generated by either an intermediary entity or the token database.

[0229] Preferably a tokenised message is generated by a bi-directional communication process.

[0230] Preferably the bi-directional communication process is between the token database and an intermediary entity.

[0231] Preferably a step in producing a tokenised message involves de-identifying data.

[0232] Preferably a step in producing a tokenised message involves adding a data element to the message.

[0233] Preferably a step in producing a tokenised message involves removing a data element from the message.

[0234] Preferably a step in producing a tokenised message involves applying an algorithm to the data elements in the message.

[0235] Preferably the token database sequences the tokenised messages.

[0236] Preferably the token database sequences the tokenised messages and transmits the tokenised messages as payment data records to a blockchain settlement system.

[0237] Preferably the blockchain settlement system employs the Ripple protocol.

[0238] Preferably the tokenised message includes at least a first data element, a second data element and a third data element.

[0239] Preferably the first data element comprises identification data for a payor, the second data element comprises identification data for a payee (biller) and the third data element comprises identification currency, denomination and value data.

[0240] Preferably a further tokenised message is generated by either an intermediary entity or the token database.

[0241] Preferably a tokenised message is generated by a bi-directional communication process.

[0242] Preferably the bi-directional communication process is between the token database and an intermediary entity.

[0243] Preferably a step in producing a tokenised message involves de-identifying data.

[0244] Preferably a step in producing a tokenised message involves adding a data element to the message.

[0245] Preferably a step in producing a tokenised message involves removing a data element from the message.

[0246] Preferably a step in producing a tokenised message involves applying an algorithm to the data elements in the message.

[0247] Preferably the token database sequences the tokenised messages.

[0248] Preferably the token database sequences the tokenised messages and transmits the tokenised messages as payment data records to a blockchain settlement system.

[0249] Preferably the blockchain settlement system employs the Ripple protocol.

[0250] Preferably a second message is transmitted between the intermediaries.

[0251] Preferably the second message is tokenised.

[0252] Preferably the second message contains conventional data.

[0253] Preferably the second message is transmitted by means of a blockchain system.

[0254] Preferably the second message includes information equivalent to that transmitted by the SWIFT system.

[0255] Preferably the tokenised message includes additional information beyond that transmitted by the SWIFT system.

[0256] The system wherein the tokenised message includes information which verifies the security status of at least one party to the financial transaction.

[0257] Preferably the second tokenised message includes information which verifies the security status of both parties to the financial transaction.

[0258] Preferably the token is conveyed by way of a medium utilizing the SWIFT messaging system or other compatible messaging system.

[0259] Preferably the medium is implemented by way of a VPN.

[0260] Preferably deidentified data associated with the financial transaction to which the token pertains is transmitted over a separate communication medium.

[0261] Preferably the separate communication medium utilizes a blockchain structure.

[0262] Preferably the deidentified data is located within a record structure which is replicated throughout the blockchain structure.

[0263] Preferably in use a sellers bank as part of entering into the financial transaction with buyers bank will establish a SWIFT transaction.

[0264] Preferably in parallel the sellers bank will perform associated operations needed to complete the financial transaction such as verification of the buyers ID and related characteristics.

[0265] Preferably data related to the associated operations is then placed in a record structure and that record is placed into the blockchain structure.

[0266] Preferably the associated data includes deidentifed data.

[0267] Preferably the data is available to the buyers bank by way of the buyers bank logging into the blockchain structure and receiving the deidentified data which is associated with the financial transaction which is represented by the token thereby allowing assembly by the buyers bank of all necessary data to execute the financial transaction on behalf of the buyer and seller.

[0268] Preferably incorporating secure channels thereby permitting only selected entities to communicate the data to execute the financial transaction on behalf of the buyer and seller.

Advantages

[0269] The invention is not limited to interaction between two banks only, but can be extended to any number of banks involved in the financial transaction. For example, the token can be included in all the financial messages sent between a plurality of banks, and the token can be used by any bank from the plurality of banks to verify the financial transaction from the enriched data record, before taking any further steps in the process.

[0270] The messaging bus allows all the financial institutions involved in the financial transaction to communicate in real-time and ensure that the payer, the beneficiary, and all the parameters corresponding to the financial transaction are validated. Further, encryption/decryption of the requests

and responses using asymmetrical pairs of keys ensures that the transmission of the request and the responses is always secure. Further, the payment risk rating ensures better straight through processing by reducing exceptions and false positives. Also, the token is compatible with a large array of formats, including JSON, XML, CSV, SWIFT, over a number of transports, including HTTP, FTP, AMQP, and JMS.

Interpretation

[0271] Unless otherwise defined, all terms (including technical and scientific terms) used herein have the same meaning as commonly understood by one of ordinary skill in the art to which this invention belongs. It will be further understood that terms used herein should be interpreted as having a meaning that is consistent with their meaning in the context of this specification and the relevant art and will not be interpreted in an idealized or overly formal sense unless expressly so defined herein. For the purposes of the present invention, additional terms are defined below. Furthermore, all definitions, as defined and used herein, should be understood to control over dictionary definitions, definitions in documents incorporated by reference, and/or ordinary meanings of the defined terms unless there is doubt as to the meaning of a particular term, in which case the common dictionary definition and/or common usage of the term will prevail.

[0272] The terminology used herein is for the purpose of describing particular embodiments only and is not intended to be limiting of the invention. As used herein, the singular articles “a”, “an” and “the” are intended to include the plural forms as well, unless the context clearly indicates otherwise and thus are used herein to refer to one or to more than one (i.e. to “at least one”) of the grammatical object of the article. By way of example, the phrase “an element” refers to one element or more than one element.

[0273] The term "about" is used herein to refer to quantities that vary by as much as 30%, preferably by as much as 20%, and more preferably by as much as 10% to a reference quantity. The use of the word 'about' to qualify a number is merely an express indication that the number is not to be construed as a precise value.

[0274] Throughout this specification, unless the context requires otherwise, the words "comprise", "comprises" and "comprising" will be understood to imply the inclusion of a stated step or element or group of steps or elements but not the exclusion of any other step or element or group of steps or elements.

[0275] The term "real-time" for example "displaying real-time data," refers to the display of the data without intentional delay, given the processing limitations of the system and the time required to accurately measure the data.

[0276] As used herein, the term "exemplary" is used in the sense of providing examples, as opposed to indicating quality. That is, an "exemplary embodiment" is an embodiment provided as an example, as opposed to necessarily being an embodiment of exemplary quality for example serving as a desirable model or representing the best of its kind.

[0277] The phrase "and/or," as used herein in the specification and in the claims, should be understood to mean "either or both" of the elements so conjoined, i.e., elements that are conjunctively present in some cases and disjunctively present in other cases. Multiple elements listed with "and/or" should be construed in the same fashion, i.e., "one or more" of the elements so conjoined. Other elements may optionally be present other than the elements specifically identified by the "and/or" clause, whether related or unrelated to those elements specifically identified. Thus, as a non-limiting example, a reference to "A and/or B", when used in conjunction with open-

ended language such as "comprising" can refer, In one embodiment of the invention, to A only (optionally including elements other than B); in another embodiment, to B only (optionally including elements other than A); in yet another embodiment, to both A and B (optionally including other elements); etc.

[0278] As used herein in the specification and in the claims, "or" should be understood to have the same meaning as "and/or" as defined above. For example, when separating items in a list, "or" or "and/or" shall be interpreted as being inclusive, i.e., the inclusion of at least one, but also including more than one, of a number or list of elements, and, optionally, additional unlisted items. Only terms clearly indicated to the contrary, such as "only one of" or "exactly one of," or, when used in the claims, "consisting of" will refer to the inclusion of exactly one element of a number or list of elements. In general, the term "or" as used herein shall only be interpreted as indicating exclusive alternatives (i.e. "one or the other but not both") when preceded by terms of exclusivity, such as "either," "one of," "only one of," or "exactly one of." "Consisting essentially of," when used in the claims, shall have its ordinary meaning as used in the field of patent law.

[0279] As used herein in the specification and in the claims, the phrase "at least one," in reference to a list of one or more elements, should be understood to mean at least one element selected from any one or more of the elements in the list of elements, but not necessarily including at least one of each and every element specifically listed within the list of elements and not excluding any combinations of elements in the list of elements. This definition also allows that elements may optionally be present other than the elements specifically identified within the list of elements to which the phrase "at least one" refers, whether related or unrelated to those elements specifically identified. Thus, as a non-limiting example, "at least one of A and B" (or, equivalently, "at least one of A or B," or, equivalently "at least one of A

and/or B") can refer, In one embodiment of the invention, to at least one, optionally including more than one, A, with no B present (and optionally including elements other than B); in another embodiment, to at least one, optionally including more than one, B, with no A present (and optionally including elements other than A); in yet another embodiment, to at least one, optionally including more than one, A, and at least one, optionally including more than one, B (and optionally including other elements); etc.

Bus

[0280] In the context of this document, the term "bus" and its derivatives, while being described in a preferred embodiment as being a communication bus subsystem for interconnecting various devices including by way of parallel connectivity such as Industry Standard Architecture (ISA), conventional Peripheral Component Interconnect (PCI) and the like or serial connectivity such as PCI Express (PCIe), Serial Advanced Technology Attachment (Serial ATA) and the like, should be construed broadly herein as any system for communicating data.

In accordance with:

[0281] As described herein, 'in accordance with' may also mean 'as a function of' and is not necessarily limited to the integers specified in relation thereto.

Composite items

[0282] As described herein, 'a computer implemented method' should not necessarily be inferred as being performed by a single computing device such that the steps of the computer implemented method may be performed by more than one cooperating computing devices.

[0283] Similarly objects as used herein such as 'web server', 'server', 'client computing device', 'computer readable medium' and the like should not necessarily be construed as being a single object, and may be implemented as a two or more objects in cooperation, such as, for example, a web server

being construed as two or more web servers in a server farm cooperating to achieve a desired goal or a computer readable medium being distributed in a composite manner, such as program code being provided on a compact disk activatable by a license key downloadable from a computer network.

Database:

[0284] In the context of this document, the term "database" and its derivatives may be used to describe a single database, a set of databases, a system of databases or the like. The system of databases may comprise a set of databases wherein the set of databases may be stored on a single implementation or span across multiple implementations. The term "database" is also not limited to refer to a certain database format rather may refer to any database format. For example, database formats may include MySQL, MySQLi , XML or the like.

Wireless:

[0285] The invention may be embodied using devices conforming to other network standards and for other applications, including, for example other WLAN standards and other wireless standards. Applications that can be accommodated include IEEE 802.11 wireless LANs and links, and wireless Ethernet.

[0286] In the context of this document, the term "wireless" and its derivatives may be used to describe circuits, devices, systems, methods, techniques, communications channels, etc., that may communicate data through the use of modulated electromagnetic radiation through a non-solid medium. The term does not imply that the associated devices do not contain any wires, although in some embodiments they might not. In the context of this document, the term "wired" and its derivatives may be used to describe circuits, devices, systems, methods, techniques, communications channels, etc., that may communicate data through the use of modulated

electromagnetic radiation through a solid medium. The term does not imply that the associated devices are coupled by electrically conductive wires.

Processes:

[0287] Unless specifically stated otherwise, as apparent from the following discussions, it is appreciated that throughout the specification discussions utilizing terms such as "processing", "computing", "calculating", "determining", "analysing" or the like, refer to the action and/or processes of a computer or computing system, or similar electronic computing device, that manipulate and/or transform data represented as physical, such as electronic, quantities into other data similarly represented as physical quantities.

Processor:

[0288] In a similar manner, the term "processor" may refer to any device or portion of a device that processes electronic data, e.g., from registers and/or memory to transform that electronic data into other electronic data that, e.g., may be stored in registers and/or memory. A "computer" or a "computing device" or a "computing machine" or a "computing platform" may include one or more processors.

[0289] The computer implemented methodologies described herein are, In one embodiment of the invention, performable by one or more processors that accept computer-readable (also called machine-readable) code containing a set of instructions that when executed by one or more of the processors carry out at least one of the computer implemented methods described herein. Any processor capable of executing a set of instructions (sequential or otherwise) that specify actions to be taken are included. Thus, one example is a typical processing system that includes one or more processors. The processing system further may include a memory subsystem including main RAM and/or a static RAM, and/or ROM.

Computer-Readable Medium:

[0290] Furthermore, a computer-readable carrier medium may form, or be included in a computer program product. A computer program product can be stored on a computer usable carrier medium, the computer program product comprising a computer readable program means for causing a processor to perform a method as described herein.

Networked or Multiple Processors:

[0291] In alternative embodiments, the one or more processors operate as a standalone device or may be connected, e.g., networked to other processor(s), in a networked deployment, the one or more processors may operate in the capacity of a server or a client machine in server-client network environment, or as a peer machine in a peer-to-peer or distributed network environment. The one or more processors may form a web appliance, a network router, switch or bridge, or any machine capable of executing a set of instructions (sequential or otherwise) that specify actions to be taken by that machine.

[0292] Note that while some diagram(s) only show(s) a single processor and a single memory that carries the computer-readable code, those in the art will understand that many of the components described above are included, but not explicitly shown or described in order not to obscure the inventive aspect. For example, while only a single machine is illustrated, the term "machine" shall also be taken to include any collection of machines that individually or jointly execute a set (or multiple sets) of instructions to perform any one or more of the computer implemented methodologies discussed herein.

Additional Embodiments:

[0293] Thus, one embodiment of each of the computer implemented methods described herein is in the form of a computer-readable carrier medium

carrying a set of instructions, e.g., a computer program that are for execution on one or more processors. Thus, as will be appreciated by those skilled in the art, embodiments of the present invention may be embodied as a method, an apparatus such as a special purpose apparatus, an apparatus such as a data processing system, or a computer-readable carrier medium. The computer-readable carrier medium carries computer readable code including a set of instructions that when executed on one or more processors cause a processor or processors to implement a method. Accordingly, aspects of the present invention may take the form of a method, an entirely hardware embodiment, an entirely software embodiment or an embodiment combining software and hardware aspects. Furthermore, the present invention may take the form of carrier medium (e.g., a computer program product on a computer-readable storage medium) carrying computer-readable program code embodied in the medium.

Carrier Medium:

[0294] The software may further be transmitted or received over a network via a network interface device. While the carrier medium is shown in an example embodiment to be a single medium, the term "carrier medium" should be taken to include a single medium or multiple media (e.g., a centralized or distributed database, and/or associated caches and servers) that store the one or more sets of instructions. The term "carrier medium" shall also be taken to include any medium that is capable of storing, encoding or carrying a set of instructions for execution by one or more of the processors and that cause the one or more processors to perform any one or more of the computer implemented methodologies of the present invention. A carrier medium may take many forms, including but not limited to, non-volatile media, volatile media, and transmission media.

Implementation:

[0295] It will be understood that the steps of methods discussed are performed In one embodiment of the invention by an appropriate processor (or processors) of a processing (i.e., computer) system executing instructions (computer-readable code) stored in storage. It will also be understood that the invention is not limited to any particular implementation or programming technique and that the invention may be implemented using any appropriate techniques for implementing the functionality described herein. The invention is not limited to any particular programming language or operating system.

Means For Carrying out a Method or Function

[0296] Furthermore, some of the embodiments are described herein as a method or combination of elements of a method that can be implemented by a processor of a processor device, computer system, or by other means of carrying out the function. Thus, a processor with the necessary instructions for carrying out such a method or element of a method forms a means for carrying out the computer implemented method or element of a method. Furthermore, an element described herein of an apparatus embodiment is an example of a means for carrying out the function performed by the element for the purpose of carrying out the invention.

Connected

[0297] Similarly, it is to be noticed that the term connected, when used in the claims, should not be interpreted as being limitative to direct connections only. Thus, the scope of the expression a device A connected to a device B should not be limited to devices or systems wherein an output of device A is directly connected to an input of device B. It means that there exists a path between an output of A and an input of B which may be a path including other devices or means. "Connected" may mean that two or more elements are either in direct physical or electrical contact, or that two or more

elements are not in direct contact with each other but yet still co-operate or interact with each other.

Embodiments:

[0298] Reference throughout this specification to "one embodiment" or "an embodiment" means that a particular feature, structure or characteristic described in connection with the embodiment is included in at least one embodiment of the present invention. Thus, appearances of the phrases "In one embodiment of the invention" or "in an embodiment" in various places throughout this specification are not necessarily all referring to the same embodiment, but may. Furthermore, the particular features, structures or characteristics may be combined in any suitable manner, as would be apparent to one of ordinary skill in the art from this disclosure, in one or more embodiments.

[0299] Similarly it should be appreciated that in the above description of example embodiments of the invention, various features of the invention are sometimes grouped together in a single embodiment, figure, or description thereof for the purpose of streamlining the disclosure and aiding in the understanding of one or more of the various inventive aspects. This method of disclosure, however, is not to be interpreted as reflecting an intention that the claimed invention requires more features than are expressly recited in each claim. Rather, as the following claims reflect, inventive aspects lie in less than all features of a single foregoing disclosed embodiment. Thus, the claims following the Detailed Description of Specific Embodiments are hereby expressly incorporated into this Detailed Description of Specific Embodiments, with each claim standing on its own as a separate embodiment of this invention.

[0300] Furthermore, while some embodiments described herein include some but not other features included in other embodiments, combinations of

features of different embodiments are meant to be within the scope of the invention, and form different embodiments, as would be understood by those in the art. For example, in the following claims, any of the claimed embodiments can be used in any combination.

Specific Details

[0301] In the description provided herein, numerous specific details are set forth. However, it is understood that embodiments of the invention may be practiced without these specific details. In other instances, well-known methods, structures and techniques have not been shown in detail in order not to obscure an understanding of this description.

[0302] It will be appreciated that the computer implemented methods and systems described/illustrated above at least substantially provides a manner in which data generated in an EHR, during an episode of care, may be de-identified (or anonymized) and provided to a user through a secure channel.

[0303] The embodiments described herein, and/or shown in the drawings, are presented by way of example only and are not limiting as to the scope of the invention. Unless otherwise specifically stated, individual aspects and components of the embodiments may be modified, or may have been substituted therefore known equivalents, or as yet unknown substitutes such as may be developed in the future or such as may be found to be acceptable substitutes in the future. The embodiments may also be modified for a variety of applications while remaining within the scope and spirit of the claimed invention, since the range of potential applications is great, and since it is intended that the present invention be adaptable to many such variations.

Different Instances of Objects

[0304] As used herein, unless otherwise specified the use of the ordinal adjectives "first", "second", "third", etc., to describe a common object, merely indicate that different instances of like objects are being referred to, and are not intended to imply that the objects so described must be in a given sequence, either temporally, spatially, in ranking, or in any other manner.

Comprising and Including

[0305] In the claims which follow and in the preceding description of the invention, except where the context requires otherwise due to express language or necessary implication, the word "comprise" or variations such as "comprises" or "comprising" are used in an inclusive sense, i.e. to specify the presence of the stated features but not to preclude the presence or addition of further features in various embodiments of the invention.

[0306] Any one of the terms: including or which includes or that includes as used herein is also an open term that also means including at least the elements/features that follow the term, but not excluding others. Thus, including is synonymous with and means comprising.

Scope of Invention

[0307] Thus, while there has been described what are believed to be the preferred embodiments of the invention, those skilled in the art will recognize that other and further modifications may be made thereto without departing from the spirit of the invention, and it is intended to claim all such changes and modifications as fall within the scope of the invention. For example, any formulas given above are merely representative of procedures that may be used. Functionality may be added or deleted from the block diagrams and operations may be interchanged among functional blocks. Steps may be added or deleted to methods described within the scope of the present invention.

[0308] Although the invention has been described with reference to specific examples, it will be appreciated by those skilled in the art that the invention may be embodied in many other forms.

Chronological order

[0309] For the purpose of this specification, where method steps are described in sequence, the sequence does not necessarily mean that the steps are to be carried out in chronological order in that sequence, unless there is no other logical manner of interpreting the sequence.

Industrial Applicability

[0310] It is apparent from the above, that the arrangements described are applicable to the industries dealing with banking, brokerages, insurance companies, investment companies and Unit Investment Trusts (UIT) etc.

Examples of tokenised messages and their generation and transmission

The previous, meta-data mode is first. It switches to minimal half way through

--

Bank:HSBC >> createUserCode >> Sparro:Sparro

{"id":"User:ABC Paper","name":"ABC Paper"}

(Creating Sparro User Code - Meta-data given can be used by other banks for compliance and for confirming payee with customers.)

--

Bank:MayBank >> createUserCode >> Sparro:Sparro

{"id":"User:XYZ Printing","name":"XYZ Printing"}

(Creating Sparro User Code - Meta-data given can be used by other banks for compliance and for confirming payee with customers.)

--

Sparro:Sparro >> createUserCode-reply >> Bank:HSBC

{"id":"User:ABC Paper","name":"ABC Paper","code":"65q3gdd"}

--

Sparro:Sparro >> createUserCode-reply >> Bank:MayBank

{"id":"User:XYZ Printing","name":"XYZ Printing","code":"70wqgx6"}

--

User:ABC Paper >> createInvoice >> Bank:HSBC

{"amount":{"amount":1000,"currency":"gbp"}}

--

Bank:HSBC >> createInvoiceCode >> Sparro:Sparro

{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd"}

(Creating Invoice Code - An invoice code is created by Sparro and connected to the bank.)

-

Sparro:Sparro >> createInvoiceCode-reply >> Bank:HSBC

{"code":"6tq6wcbad"}

--

Bank:HSBC >> createInvoice-reply >> User:ABC Paper
{"invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":
"65q3gdd","code":"6tq6wcbad"}}

Abc invoice { amount: { amount: 1000, currency: 'gbp' },
payee: '65q3gdd',
code: '6tq6wcbad' }
--
User:ABC Paper >> invoice >> User:XYZ Printing
{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":
"6tq6wcbad"}
-
User:XYZ Printing >> payInvoice >> Bank:MayBank
{"invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300}}
--
Bank:MayBank >> sendMoney >> BankGateway:MayBank
{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP",
"amount":300}}
--
BankGateway:MayBank >> getInvoice >> Sparro:Sparro
"6tq6wcbad"
(Sending Payment to Invoice - The payment is sent to the bank
that created the invoice.)
--
Sparro:Sparro >> getInvoice-reply >> BankGateway:MayBank
{"bank":"Bank:HSBC","invoice":{"amount":{"amount":1000,"currency":
"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}
--
BankGateway:MayBank >> transfer >> BankGateway:HSBC
{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP",
"amount":300},"id":"ripple-1"}

--
BankGateway:HSBC >> incomingTransfer >> Bank:HSBC
{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP",
"amount":300},"id":"ripple-1"}
--
BankGateway:HSBC >> transfer-reply >> BankGateway:MayBank
{"success":true,"owed":{"GBP":300}}
--
Bank:HSBC >> getInvoice >> Sparro:Sparro
"6tq6wcbad"
--
BankGateway:MayBank >> sendMoney-reply >> Bank:MayBank
{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP",
"amount":300},"id":"ripple-1"}
--
Sparro:Sparro >> getInvoice-reply >> Bank:HSBC
{"bank":"Bank:HSBC","invoice":{"amount":{"amount":1000,"currency":
"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}
--
Bank:MayBank >> payInvoice-reply >> User:XYZ Printing
{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP",
"amount":300},"id":"ripple-1"}

XYZ part-paid invoice {
"payer": "70wqgx6",
"invoice": "6tq6wcbad",
"amount": {
"currency": "GBP",
"amount": 300
},
"id": "ripple-1"

--

Bank:HSBC >> incomingTransfer >> User:ABC Paper

{"invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":
"65q3gdd","code":"6tq6wcbad"},"transfer":{"payer":"70wqgx6","invoice":
"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":"ripple-1"}}

-

User:XYZ Printing >> payInvoice >> Bank:MayBank

{"invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700}}

--

Bank:MayBank >> sendMoney >> BankGateway:MayBank

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP",
"amount":700}}

--

BankGateway:MayBank >> getInvoice >> Sparro:Sparro

"6tq6wcbad"

(Sending Payment to Invoice - The payment is sent to the bank
that created the invoice.)

--

Sparro:Sparro >> getInvoice-reply >> BankGateway:MayBank

{"bank":"Bank:HSBC","invoice":{"amount":{"amount":1000,
"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

--

BankGateway:MayBank >> transfer >> BankGateway:HSBC

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":
{"currency":"GBP","amount":700},"id":"ripple-2"}

--

BankGateway:HSBC >> incomingTransfer >> Bank:HSBC

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":
{"currency":"GBP","amount":700},"id":"ripple-2"}

--

BankGateway:HSBC >> transfer-reply >> BankGateway:MayBank

{"success":true,"owed":{"GBP":1000}}
--
Bank:HSBC >> getInvoice >> Sparro:Sparro
"6tq6wcbad"
-
BankGateway:MayBank >> sendMoney-reply >> Bank:MayBank
{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":
{"currency":"GBP","amount":700},"id":"ripple-2"}
--
Sparro:Sparro >> getInvoice-reply >> Bank:HSBC
{"bank":"Bank:HSBC","invoice":{"amount":{"amount":
1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}
--
Bank:MayBank >> payInvoice-reply >> User:XYZ Printing
{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":
{"currency":"GBP","amount":700},"id":"ripple-2"}
XYZ finished paying invoice {
"payer": "70wqgx6",
"invoice": "6tq6wcbad",
"amount": {
"currency": "GBP",
"amount": 700
},
"id": "ripple-2"
}
--- SWITCHING TO MODE: minimal ---
--
Bank:HSBC >> incomingTransfer >> User:ABC Paper
{"invoice":{"amount":{"amount":1000,"currency":"gbp"},
"payee":"65q3gdd","code":"6tq6wcbad"},"transfer":
{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":

{"currency":"GBP","amount":700},"id":"ripple-2"}}

--Bank:HSBC >> createUserCode >> Sparro:Sparro

undefined

(Creating Sparro User Code - No meta-data is required.)

--

Bank:MayBank >> createUserCode >> Sparro:Sparro

undefined

(Creating Sparro User Code - No meta-data is required.)

--

Sparro:Sparro >> createUserCode-reply >> Bank:HSBC

{"code":"dnt7gec"}

--

Sparro:Sparro >> createUserCode-reply >> Bank:MayBank

{"code":"6wwpwuc"}

--

User:ABC Paper >> createInvoice >> Bank:HSBC

{"amount":{"amount":2000,"currency":"gbp"}}

--

Bank:HSBC >> createInvoiceCode >> Sparro:Sparro

null

(Creating Invoice Code - An invoice code is created by Sparro and connected to the bank. No invoice details are required.)

--

Sparro:Sparro >> createInvoiceCode-reply >> Bank:HSBC

{"code":"erwkax1md"}

--Bank:HSBC >> createInvoice-reply >> User:ABC Paper

{"invoice":{"amount":{"amount":2000,"currency":"gbp"},
"code":"erwkax1md","payee":"User:ABC Paper","transfers":[]}}

Abc invoice { amount: { amount: 2000, currency: 'gbp' },
code: 'erwkax1md',
payee: 'User:ABC Paper',

transfers: [] }

--

User:ABC Paper >> invoice >> User:XYZ Printing

{"amount":{"amount":2000,"currency":"gbp"},"code":
"erwkax1md","payee":"User:ABC Paper","transfers":[]}

--

User:XYZ Printing >> payInvoice >> Bank:MayBank

{"invoice":"erwkax1md","amount":{"currency":"GBP","amount":600}}

--

Bank:MayBank >> sendMoney >> BankGateway:MayBank

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":
{"currency":"GBP","amount":600}}

--

BankGateway:MayBank >> getInvoice >> Sparro:Sparro

"erwkax1md"

(Sending Payment to Invoice - The payment is sent to the bank
that created the invoice.)

--

Sparro:Sparro >> getInvoice-reply >> BankGateway:MayBank

{"bank":"Bank:HSBC"}

--

BankGateway:MayBank >> transfer >> BankGateway:HSBC

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":
{"currency":"GBP","amount":600},"id":"ripple-3"}

--

BankGateway:HSBC >> incomingTransfer >> Bank:HSBC

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":
{"currency":"GBP","amount":600},"id":"ripple-3"}

--

BankGateway:HSBC >> transfer-reply >> BankGateway:MayBank

{"success":true,"owed":{"GBP":600}}

--

Bank:HSBC >> incomingTransfer >> User:ABC Paper

{"invoice":{"amount":{"amount":2000,"currency":"gbp"},"code":
"erwkax1md","payee":"User:ABC
Paper","transfers":[{"payer":"6wwpwuc","invoice":
"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-
3"}]},"transfer":{"payer":"6wwpwuc","invoice":"erwkax1md",
"amount":{"currency":"GBP","amount":600},"id":"ripple-3"}}

--

BankGateway:MayBank >> sendMoney-reply >> Bank:MayBank

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":
{"currency":"GBP","amount":600},"id":"ripple-3"}

--

Bank:MayBank >> payInvoice-reply >> User:XYZ Printing

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":
{"currency":"GBP","amount":600},"id":"ripple-3"}

XYZ part-paid invoice {

"payer": "6wwpwuc",

"invoice": "erwkax1md",

"amount": {

"currency": "GBP",

"amount": 600

},

"id": "ripple-3"

}

--

User:XYZ Printing >> payInvoice >> Bank:MayBank

{"invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400}}

--

Bank:MayBank >> sendMoney >> BankGateway:MayBank

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":

{"currency":"GBP","amount":1400}}
--
BankGateway:MayBank >> getInvoice >> Sparro:Sparro
"erwkax1md"
(Sending Payment to Invoice - The payment is sent to the bank that created the invoice.)
--
Sparro:Sparro >> getInvoice-reply >> BankGateway:MayBank
{"bank":"Bank:HSBC"}
-
BankGateway:MayBank >> transfer >> BankGateway:HSBC
{"payer":"6wwpwuc","invoice":"erwkax1md","amount":
{"currency":"GBP","amount":1400},"id":"ripple-4"}
--
BankGateway:HSBC >> incomingTransfer >> Bank:HSBC
{"payer":"6wwpwuc","invoice":"erwkax1md","amount":
{"currency":"GBP","amount":1400},"id":"ripple-4"}
BankGateway:HSBC >> transfer-reply >> BankGateway:MayBank
{"success":true,"owed":{"GBP":2000}}
--
Bank:HSBC >> incomingTransfer >> User:ABC Paper
{"invoice":{"amount":{"amount":2000,"currency":"gbp"},"code":
"erwkax1md","payee":"User:ABC
Paper","transfers":[{"payer":"6wwpwuc","invoice":"erwkax1md",
"amount":{"currency":"GBP","amount":600},"id":"ripple-
3"},{"payer":"6wwpwuc","invoice":"erwkax1md","amount":
{"currency":"GBP","amount":1400},"id":"ripple-
4"}]},"transfer":{"payer":"6wwpwuc","invoice":"erwkax1md",
"amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}}
--
BankGateway:MayBank >> sendMoney-reply >> Bank:MayBank

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":
{"currency":"GBP","amount":1400},"id":"ripple-4"}
--
Bank:MayBank >> payInvoice-reply >> User:XYZ Printing
{"payer":"6wwpwuc","invoice":"erwkax1md","amount":
{"currency":"GBP","amount":1400},"id":"ripple-4"}
XYZ finished paying invoice {
"payer": "6wwpwuc",
"invoice": "erwkax1md",
"amount": {
"currency": "GBP",
"amount": 1400
},
"id": "ripple-4"
}

Electronic Acknowledgement Receipt

EFS ID:	41556115
Application Number:	15752711
International Application Number:	
Confirmation Number:	5327
Title of Invention:	COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR
First Named Inventor/Applicant Name:	Nick Armstrong
Customer Number:	23117
Filer:	Alan Mark Kagen/Janet Stoy
Filer Authorized By:	Alan Mark Kagen
Attorney Docket Number:	AMK-5243-9
Receipt Date:	05-JAN-2021
Filing Date:	14-FEB-2018
Time Stamp:	13:06:41
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		5243-9_rule_312_amd_and_substitute_spec_marked_up.pdf	502877 19ec00e52ac04e6d73b7a1857fce6f52bff5b5f2	yes	102

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment after Notice of Allowance (Rule 312)	1	1
	Specification	2	2
	Applicant Arguments/Remarks Made in an Amendment	3	102

Warnings:

Information:

2	Specification	5243-9_substitute_spec_clean_copy.pdf	348146 2c9e841ea75f643b83194b2f705bd39c6a30a7ba	no	86

Warnings:

Information:

Total Files Size (in bytes):	851023

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

23117 7590 12/02/2020

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER
ABDULLAEV, AMANULLA

ART UNIT	PAPER NUMBER
3692	

DATE MAILED: 12/02/2020

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/752,711	02/14/2018	Nick Armstrong	AMK-5243-9	5327

TITLE OF INVENTION: COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$600	$0.00	$0.00	$600	03/02/2021

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

23117 7590 12/02/2020
NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/752,711	02/14/2018	Nick Armstrong	AMK-5243-9	5327

TITLE OF INVENTION: COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$600	$0.00	$0.00	$600	03/02/2021

EXAMINER	ART UNIT	CLASS-SUBCLASS
ABDULLAEV, AMANULLA	3692	705-039000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. Fees submitted: ❑ Issue Fee ❑ Publication Fee (if required) ❑ Advance Order - # of Copies _____

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

❑ Electronic Payment via EFS-Web ❑ Enclosed check ❑ Non-electronic payment by credit card (Attach form PTO-2038)

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. **Change in Entity Status** (from status indicated above)

❑ Applicant certifying micro entity status. See 37 CFR 1.29

❑ Applicant asserting small entity status. See 37 CFR 1.27

❑ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/752,711	02/14/2018	Nick Armstrong	AMK-5243-9	5327

23117 7590 12/02/2020

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
ABDULLAEV, AMANULLA	
ART UNIT	**PAPER NUMBER**
3692	

DATE MAILED: 12/02/2020

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 15/752,711	Applicant(s) Armstrong, Nick	
	Examiner AMANULLA ABDULLAEV	Art Unit 3692	AIA (FITF) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☑ This communication is responsive to the amendment and response filed April 21, 2020.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☑ The allowed claim(s) is/are 59-78 . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

4. ☑ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☑ All b) ☐ Some *c) ☐ None of the:

   1. ☑ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☑ Notice of References Cited (PTO-892)
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____.
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date. _____.
5. ☐ Examiner's Amendment/Comment
6. ☑ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/AMANULLA ABDULLAEV/ Examiner, Art Unit 3692	/ELIZABETH H ROSEN/ Primary Examiner, Art Unit 3692

DETAILED ACTION

Status of Application

This action is in reply to the amendment and response to filed on April 21, 2020.

Claims 59 and 62 have been amended.

Claims 59-78 are pending and allowed.

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA. In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

Allowable Subject Matter

Claims 59-78 are allowed.

Claim Analysis under 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

The claims 59-78 are being analyzed according to the 2019 Revised Patent Subject Matter Eligibility Guidance (Federal Register, Vol. 84, No. 5, p.p. 50-57 (Jan. 7, 2019)).

2019 PEG Step	**Analysis of Claims 59 – 78**

Step 1: Does the Claim Fall Within a Statutory Category?	Yes. Claims 59-72 recite a method and, therefore, directed to the statutory class of process. Claim 73 recites a system and, therefore, are directed to the statutory class of machine or manufacture. Claims 74-78 recite an intermediary server and, therefore, are directed to the statutory class of machine.
Step 2A, Prong 1: Is a Judicial Exception Recited?	Yes. But for the computer components (i.e., additional elements), the claims as a whole recite a method of organizing human activity. The claims are directed to a method and system for transmitting all kind of data pertaining to financial transactions. This type of method of organizing human activity is similar to a commercial interactions such as sales activities, business relations. Thus, the claims recite an abstract idea.
Step 2A, Prong 2: Is the Abstract Idea Integrated into a Practical Application?	Yes. The claims recite a combination of additional elements including transmitting financial documents, generating an enriched data record, requesting generation of a token for identifying the financial documents, generating the token at the token server and adding it into the blockchain, transmitting the token to the intermediary server from the token server, and transmitting the token from the intermediary server to the document store. The claim as whole integrates the method of organizing human activity into a practical application. Specifically, the additional elements recite a specific improvement over prior art systems by using the multiple transmissions of the token to secure the financial transaction. Thus, the claims are **eligible** because they are not directed to the recited judicial exception (abstract idea).
Step 2B: Does the Claim Provide an Inventive Concept?	**N/A.**

Reasons for Allowance

The following is an examiner's statement of reasons for allowance:

One of the closest prior art references of record is Witchey, U.S. Patent Application Publication No. US 2015/0332283 A1. Witchey teaches that the doctor performs services for the patient, information related to the services (e.g., inputs, outputs, codes, etc.) are packaged in the form of a healthcare transaction, the information can be considered to represent input information related to the healthcare transaction in progress, the actions taken by the doctor can be considered outputs to or outcomes of the healthcare transaction, managing healthcare transactions in the form of healthcare blockchains, the various attributes or properties of the inputs and outputs can be represented by healthcare tokens, the healthcare transaction represented by healthcare tokens among other pieces of information, the transaction could include a transaction ID, a time stamp, validator digital signature, or other data. However, Witchey does not teach the financial transactions and implementing a smart contract.

Another of the closest prior art references of record is Davis, U.S. Patent Application Publication No. US 2016/0342994 A1. Davis teaches storing blockchain transaction related information in traditional payment systems in order to leverage the capabilities of the traditional payment networks, during blockchain transactions happening on a blockchain network and storing the private key on behalf of the payer and configured to generate the digital signature and include the generated signature and transaction identifier in transaction messages for blockchain transactions involving the payer.

Another of the closest prior art references of record is Morgan, U.S. Patent Application Publication No. US 2012/0203665 A1. Morgan teaches that a document pertaining to a financial transaction is saved in a first document store, QR code indicative of a financial payment may be sent from a centralized financial system to the device of a first user and shared with a second user, the payment processor saves a receipt of the transaction in the purchase history database,

QR code, may be generated by a backend server and sent to POS device for presentation to a customer.

Another of the closest prior art references of record is Castinado, U.S. Patent Application Publication No. US 20170132630 A1. Castinado teaches that smart contracts engine is provided for implementing smart contracts for managing alias-token selection for processing payments, smart contract infrastructure can be implemented by replicated asset registries and contract execution using cryptographic hash chains and Byzantine fault tolerant replication, and adding the smart contract into the blockchain.

Another of the closest prior art references of record is Matsuo, U.S. Patent Application Publication No. US 2009/0307495 A1. Matsuo teaches that a request with its appropriate keys may be encrypted and decrypted for security.

Another of the closest prior art references of record is Pennanen, U.S. Patent No. 10,346,814. Pennanen teaches that a first public key and second public key for two transacting parties are added to the blockchain from different servers.

Another of the closest prior art references of record is https://fc16.ifca.ai/bitcoin (Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab, (Jan. 15, 2014).).

Another of the closest prior art references of record is Bird & Bird (Blockchain 2.0, smart contracts and challenges, (June/July 2016).).

Prior arts references teach receiving electronic payment transaction data, inputs and outputs that represented by healthcare tokens, blockchain transactions, generating digital signatures, transaction related enriched data record, implementing smart contracts related to

managing token selection for processing payments and adding the smart contract into the blockchain.

Claims 59-78 are allowed because these prior art references, for example, in claim 59 do not teach the adding the enriched data record into a blockchain being a distributed ledger, requesting generation of a token corresponding to the financial transaction to identify the documents, transmitting the token to the server, in claim 61 implementing a smart contract at the token server, in claim 73 generating an enriched data record, requesting generation of a token for identifying the financial documents, generating the token at the token server and adding it into the blockchain, transmitting the token to the intermediary server from the token server, and transmitting the token from the intermediary server to the document store. Although claim limitations can be found in prior art references, but prior art references do not disclose or make obvious the combination of claim limitations. Therefore, the rejections under 35 U.S.C. 103 have been withdrawn.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to AMANULLA ABDULLAEV whose telephone number is (571)272-4367. The examiner can normally be reached on Monday-Friday 9:30AM -4:30PM ET.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Sarah M Monfeldt can be reached on 571-270-1833. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see https://ppair-my.uspto.gov/pair/PrivatePair. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AMANULLA . ABDULLAEV
Examiner
Art Unit 3692

/ELIZABETH H ROSEN/
Primary Examiner, Art Unit 3692

Notice of References Cited	Application/Control No. 15/752,711	Applicant(s)/Patent Under Reexamination Armstrong et al.	
	Examiner AMANULLA ABDULLAEV	Art Unit 3692	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20150332283-A1	11-2015	Witchey; Nicholas J.	G06F21/645	705/3
*	B	US-20170132630-A1	05-2017	Castinado; Joseph B.	G06Q20/382	1/1
	C					
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab, https://fc16.ifca.ai/bitcoin (Year: 2014)
	V	Bird & Bird Blockchain 2.0, smart contracts and challenges, Bird & Bird; twobirds.com (Year: 2016)
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/752,711	Armstrong et al.
	Examiner	Art Unit
	AMANULLA ABDULLAEV	3692

CPC - Searched*		
Symbol	**Date**	**Examiner**
G06F 21/64	10/15/2019	JM
G06Q 20/382	10/15/2019	JM
G06Q 20/385	10/15/2019	JM
G06Q20/3674	09/21/2020	AA

CPC Combination Sets - Searched*		
Symbol	**Date**	**Examiner**

US Classification - Searched*			
Class	**Subclass**	**Date**	**Examiner**

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	**Date**	**Examiner**
Inventor search	10/15/2019	JM
EAST search history attached	10/15/2019	JM
Consulted with primary examiner Abhishek Vyas	10/15/2019	JM
Used ip.com. Screenshot attached	10/15/2019	JM
Performed EAST, GOOGLE PATENTS, IP.COM text search	09/21/2020	AA
Performed Google NPL search	10/30/2020	AA

/AMANULLA ABDULLAEV/ Examiner, Art Unit 3692	

JPMC Ex. 1002
Page 247

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/752,711	Armstrong et al.
	Examiner	Art Unit
	AMANULLA ABDULLAEV	3692

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

/AMANULLA ABDULLAEV/ Examiner, Art Unit 3692	

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/752,711	Armstrong, Nick
	Examiner	**Art Unit**
	AMANULLA ABDULLAEV	3692

CPC						
Symbol					**Type**	**Version**
G06Q	/	20	/	382	F	2013-01-01
G06F	/	21	/	64	I	2013-01-01
G06Q	/	20	/	389	I	2013-01-01
G06Q	/	20	/	3823	I	2013-01-01
G06Q	/	20	/	3827	I	2013-01-01
G06Q	/	20	/	385	I	2013-01-01
H04L	/	63	/	0442	I	2013-01-01
H04L	/	63	/	0471	I	2013-01-01

CPC Combination Sets								
Symbol					**Type**	**Set**	**Ranking**	**Version**
	/		/					

/AMANULLA ABDULLAEV/ Examiner, Art Unit 3692	07 November 2020	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	20	
/ELIZABETH H ROSEN/ Primary Examiner, Art Unit 3692	25 November 2020	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

U.S. Patent and Trademark Office — Part of Paper No.: 20200922

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/752,711	Armstrong, Nick
	Examiner	**Art Unit**
	AMANULLA ABDULLAEV	3692

INTERNATIONAL CLASSIFICATION				
CLAIMED				
G06Q	/	20	/	382
	/		/	

NON-CLAIMED				
	/		/	

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**

CROSS REFERENCES(S)						
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**					

/AMANULLA ABDULLAEV/ Examiner, Art Unit 3692	07 November 2020	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	20	
/ELIZABETH H ROSEN/ Primary Examiner, Art Unit 3692	25 November 2020	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

U.S. Patent and Trademark Office — Part of Paper No.: 20200922

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/752,711	Armstrong, Nick
	Examiner	**Art Unit**
	AMANULLA ABDULLAEV	3692

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIMS

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	59	10	68	19	77										
2	60	12	69	20	78										
3	61	13	70												
4	62	14	71												
5	63	11	72												
6	64	15	73												
7	65	16	74												
8	66	17	75												
9	67	18	76												

/AMANULLA ABDULLAEV/ Examiner, Art Unit 3692	07 November 2020	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	20	
/ELIZABETH H ROSEN/ Primary Examiner, Art Unit 3692	25 November 2020	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

U.S. Patent and Trademark Office

Part of Paper No.: 20200922

Google

financial transaction via blockchain

All | News | Images | Videos | Maps | More | Settings | Tools

Jan 1, 2000 – Aug 14, 2015 | All results | Clear

Ad · www.ibm.com/ibm_blockchain/for_finance

Blockchain Financial Services - IBM Blockchain for Finance

See How **Blockchain** Revolutionizes International Payments w/ a New Global Payment Rail. Clear & Settle Cross-Border Payments in Seconds! Discover the IBM **Blockchain** for **Finance**. Shared View of Truth. Cryptocurrency Security. Deliver Real Outcomes.

Blockchain Services
Turn Your Blockchain Strategy into Tangible Business Outcomes.

Forrester TEI Report
Download The Report To Know Your Potential ROI w/ IBM Blockchain

Blockchain For Insurance
Revolutionize The Trust that Powers Insurance with IBM Blockchain.

HFS Blockchain Report
Find Our Why IBM was Named the Flag Bearer of Enterprise Blockchain

www.bearingpoint.com › ... › Thought leadership

Can the financial services industry master blockchain ...

Aug 2, 2010 - **Blockchains** achieve the same **through** a network of participants, who validate and clear **transactions** by solving complex algorithmic puzzles. Conformance is ...

People also ask

- How Blockchain can be used in financial services?
- What is a transaction in a Blockchain?
- What is Blockchain transaction fee?
- How do I view a transaction on Blockchain?

Feedback

newagebankingsummit.com › europe › 4-key-advantag...

4 Key Advantages of Using Blockchain in Banking « New Age ...

Jan 15, 2013 - **Blockchain**, also known as distributed ledger technology, was originally developed in 2009 as a tracking database for **Bitcoin transactions**. According to IBM, 66 ...

www.wired.com › insights › 2015/01 › block-chain-2-0

Block Chain 2.0: The Renaissance of Money | WIRED

Jan 6, 2015 - Elements of Protocol Commonality: TCP/IP and the **Block Chain** ... Apart from **Financial transactions**, smart contracts are now entering the Legal System. ... Another way to look at it is that smart property can be controlled via the **Block Chain**.

www.gibsondunn.com › documents › publications › Le... PDF

Blockchain Technology and Legal Implications of - Gibson Dunn

Mar 31, 2015 - scape. Multi-Signature **Transactions**. **Financial** transfers can also be more tailored. Escrow can be accomplished via the **blockchain** by using "multi-signature ...
by JA LEE - 2015 - Cited by 5 - Related articles

www.mdpi.com › htm

Sustainability | Free Full-Text | Blockchain in FinTech: A ...

Apr 4, 2019 - A vast majority of the research is focused into finance and banking sector, obviating ... Once each node in the network verifies the information, it is sent via their public ... being the transfer of its value, started facilitating **financial transactions**.
by S Fernandez-Vazquez - 2019 - Cited by 6 - Related articles

www.ft.com › content

FT Explainer: The blockchain and financial markets | Financial ...

Jul 14, 2015 - Transactions between bitcoin users are gathered as blocks and broadcast to a network of computers. Those gathering the blocks are known as "miners", and
Missing: via | Must include: via

www.americanbanker.com › opinion › blockchain-hold...

Blockchain Holds Promise for Cross-Border Payments ...

Aug 7, 2015 - Blockchain technology may soon make the high fees, lengthy transaction times ... While financial institutions are apt to remain wary of the cryptocurrency and others ... Via Align Commerce, the U.S business sends an invoice notification to the ...

tesi.luiss.it › 682731_FINOCCHIARO_MAURIZIO_Blo... PDF

Blockchain disruption: a focus on the banking system

Feb 15, 2011 - 2.3.6 How blockchain is already impacting the Italian financial ... Participants validate the transactions through a set of rules established by the network and ...
by M Finocchiaro - 2018

www.moneycrashers.com › blockchain-technology-exp...

What Is Blockchain Technology (Explained) - How It Will Change

Nov 15, 2008 - In contrast, a digital transaction is not a physical transfer of data, but the ... technology has the power to remove the middleman in financial transactions, blur ... the Blockchain," the first DJ mix that pays the artist almost instantly via blockchain.

www.chainalysis.com

Chainalysis: The Blockchain Analysis Company

Feb 7, 2015 - Chainalysis helps government agencies, cryptocurrency businesses, and financial institutions engage confidently with cryptocurrency.

Ad · us.nttdata.com/

The Future of Banking - Solutions From NTT DATA

Reduce IT Complexity And Increase Customer Centricity As A Way Of Doing Business Right. Find The Digital Solutions To Deliver Great Customer Service And Innovative New Products
Comprehensive Portfolios. Customized Solutions. Digital Innovation Leader.
Case Studies · Public Sector Resources · Healthcare Services · Banking & Financial

Ad · www.securitize.io/

Blockchain-based securities - Tokenization & Blockchain

Use the secure power of blockchain to record ownership & transfers of digital securities. Private securities are gradually joining the digital age with blockchain and Securitize. Broker dealer suitable. Compliance. Automated Compliance. Access global capital.
Read our blogs · Contact Us · How-To Guides · Securitize Advantage

Ad · www.jpmorgan.com/

J.P. Morgan - The Future of Blockchain

Leading blockchain technology to actively develop in-house solutions. Aiming to actualize enterprise-grade blockchain tools, such as JPM Coin, IIN ® and Quorum®.
IIN® · Quorum® · JPM Coin for Payments · Next Step for Blockchain · Dromaius

Charlottesville VA, Virginia - Based on your past activity - Use precise location - Learn more

Help Send feedback Privacy Terms

Web Search History

date, time	web site	search string
9/22/2020 6:37:34 PM	Google Patents	**Keyword Group 1** [financial transaction] **Keyword Group 2** [blockchain] **Keyword Group 3** [smart contract] **Keyword Group 4** [token] **Before** Priority Date: priority:20150814 **After** Priority Date: priority:20050101

IQQueryQuickExport-202009222232

Main Concept Document
==========
US20180247302
Title: COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR

(No Concept Modifiers)
==========

(No Filters)
==========

Options
=======
De-dup: None
Cut-off: None
Sort: Relevance

Content: Patents + NPL (37)
==========
US Patents
US Designs
US Applications
EPO Patents
EPO Applications
China Patents
China Applications
Japan Patents
Japan Applications
Korea Patents
Korea Applications
WIPO Applications
IEEE Xplore Publications: IEEE Periodicals
IEEE Xplore Publications: IEEE Conferences
IEEE Xplore Publications: IEEE Standards
IEEE Xplore Publications: IEEE Early Access
IEEE Xplore Publications: IET Periodicals
IEEE Xplore Publications: IET Conferences
IEEE Xplore Publications: SMPTE Periodicals
IEEE Xplore Publications: SMPTE Conferences
IEEE Xplore Publications: SMPTE Standards
IEEE Xplore Publications: MIT Press eBooks
IEEE Xplore Publications: Wiley-IEEE eBooks
IEEE Xplore Publications: IBM Periodicals

IEEE Xplore Publications: URSI Periodicals
IEEE Xplore Publications: VDE Conferences
IEEE Xplore Publications: Periodicals from China
IP.com Prior Art Database: The IP.com Journal
IP.com Prior Art Database: Internet Society RFC
IP.com Prior Art Database: IBM TDB Archive
IP.com Prior Art Database: Legacy Journals
IP.com Prior Art Database: Software Patent Institute
OnePetro.org: Periodicals at OnePetro.org
OnePetro.org: Conferences at OnePetro.org
OnePetro.org: Standards at OnePetro.org
Other Literature: IBM Redbooks
Other Literature: PubMed Central

1.
A computer implemented method for processing a financial transaction and a system therefor
The present invention provides a computer implemented method for processing a financial transaction, the method comprising the steps of transmitting one or more documents pertaining to the financial transaction, from a first intermediary server to a first document store, generating an enriched data...
CURRENT ASSIGNEES: IDENTITII PTY LTD
5
WO2017027900A1 | WIPO APPLICATIONS | 23-FEB-2017
2.
A computer implemented method for processing a financial transaction and a system therefor
The present invention provides a computer implemented method for processing a financial transaction, the method comprising the steps of transmitting one or more documents pertaining to the financial transaction, from a first intermediary server to a first document store, generating an enriched data...
CURRENT ASSIGNEES: IDENTITII PTY LTD
5
EP3335176A1 | EPO APPLICATIONS | 20-JUN-2018
3.
System and method for generating trust tokens
A trust token may be created including authentication data for a user and his or her associated communication device. The trust token may be transmitted by the communication device to one or more recipients, such as a token server. The recipients may interpret the trust token and verify it against...
CURRENT ASSIGNEES: VISA INTL SRVC ASSOC
4
WO2019050527A1 | WIPO APPLICATIONS | 14-MAR-2019
4.
Key pair architecture for security message transmitting-receiving
The embodiment of the present invention is encrypted and is decrypted the message sent by intermediary using public private key-pair using limitation.Message may include sensitive information, and can be transmitted between entities by one or

more networks.In some embodiments, entity and/or network...
CURRENT ASSIGNEES: VISA INT SRVC ASS
4
CN110050435A | CHINA APPLICATIONS | 23-JUL-2019
5.
Key pair infrastructure for secure messaging
Embodiments of the present invention use a limited-use public/private key pair to encrypt and decrypt messages sent through an intermediary. The messages may contain sensitive information and may be transmitted between entities over one or more networks. In some embodiments, the entities and/or the...
CURRENT ASSIGNEES: VISA INTL SRVC ASSOC
4
US20180167367 | US APPLICATIONS | 14-JUN-2018
6.
Key pair infrastructure for secure messaging
Embodiments of the present invention use a limited-use public/private key pair to encrypt and decrypt messages sent through an intermediary. The messages may contain sensitive information and may be transmitted between entities over one or more networks. In some embodiments, the entities and/or the...
CURRENT ASSIGNEES: VISA INTL SRVC ASSOC
4
WO2018111727A1 | WIPO APPLICATIONS | 21-JUN-2018
7.
Key pair infrastructure for secure messaging
Embodiments of the present invention use a limited-use public/private key pair to encrypt and decrypt messages sent through an intermediary. The messages may contain sensitive information and may be transmitted between entities over one or more networks. In some embodiments, the entities and/or the...
CURRENT ASSIGNEES: JOHN RHIDIAN [+2]
4
US20190089683 | US APPLICATIONS | 21-MAR-2019
8.
Key pair infrastructure for secure messaging
Embodiments of the present invention use a limited-use public/private key pair to encrypt and decrypt messages sent through an intermediary. The messages may contain sensitive information and may be transmitted between entities over one or more networks. In some embodiments, the entities and/or the...
CURRENT ASSIGNEES: VISA INTL SRVC ASSOC
4
EP3556048A1 | EPO APPLICATIONS | 23-OCT-2019
9.
Key pair infrastructure for secure messaging
Embodiments of the present invention use a limited-use public/private key pair to encrypt and decrypt messages sent through an intermediary. The messages may contain sensitive information and may be transmitted between entities over one or more networks. In some embodiments, the entities and/or the...
CURRENT ASSIGNEES: VISA INTL SRVC ASSOC
4

US10205709 | US PATENTS | 12-FEB-2019
10.
Key pair infrastructure for secure messaging
Embodiments of the present invention use a limited-use public/private key pair to encrypt and decrypt messages sent through an intermediary. The messages may contain sensitive information and may be transmitted between entities over one or more networks. In some embodiments, the entities and/or the...
CURRENT ASSIGNEES: VISA INTL SRVC ASSOC
4
US20190288989 | US APPLICATIONS | 19-SEP-2019
11.
Key pair infrastructure for secure messaging
Embodiments of the present invention use a limited-use public/private key pair to encrypt and decrypt messages sent through an intermediary. The messages may contain sensitive information and may be transmitted between entities over one or more networks. In some embodiments, the entities and/or the...
CURRENT ASSIGNEES: VISA INTL SRVC ASSOC
4
US10356057 | US PATENTS | 16-JUL-2019
12.
Techniques for secure blockchain management
Embodiments of the invention are directed to a method for reducing a computational burden of a blockchain provider. A data processing computer may facilitate an exchange of a data transfer message between respective applications of a first and second device. The data processing computer may maintain...
CURRENT ASSIGNEES: VISA INTL SRVC ASSOC
4
US20190327218 | US APPLICATIONS | 24-OCT-2019
13.
Techniques for secure blockchain management
Embodiments of the invention are directed to a method for reducing a computational burden of a blockchain provider. A data processing computer may facilitate an exchange of a data transfer message between respective applications of a first and second device. The data processing computer may maintain...
CURRENT ASSIGNEES: VISA INTL SRVC ASSOC
4
WO2018132108A1 | WIPO APPLICATIONS | 19-JUL-2018
14.
Techniques for secure blockchain management
Embodiments of the invention are directed to a method for reducing a computational burden of a blockchain provider. A data processing computer may facilitate an exchange of a data transfer message between respective applications of a first and second device. The data processing computer may maintain...
CURRENT ASSIGNEES: VISA INTL SRVC ASSOC
4
EP3568950A1 | EPO APPLICATIONS | 20-NOV-2019
15.
Apparatus configured to facilitate secure financial transactions

An aspect provides an apparatus configured to facilitate secure financial transactions.
CURRENT ASSIGNEES: CALEDON COMPUTER SYS INC
4
WO2014089682A1 | WIPO APPLICATIONS | 19-JUN-2014
16.
Apparatus configured to facilitate secure financial transactions
An aspect provides an apparatus configured to facilitate secure financial transactions.
CURRENT ASSIGNEES: CALEDON COMPUTER SYS INC
4
US20140201084 | US APPLICATIONS | 17-JUL-2014
17.
Secure messaging system
A method for secure data transactions over a computer network is described. In one embodiment, the act of generating at the first party a document, which authorizes the data transaction to proceed is performed. In one embodiment, the document content is signed using a computer network with...
CURRENT ASSIGNEES: BUSHMAN M BENJAMIN [+4]
4
US20110208961 | US APPLICATIONS | 25-AUG-2011
18.
Secure electronic payment messaging system with reconcilable finality
A transfer network system for providing communications between commercial buyers and suppliers and their respective banks is provided. Client systems in communication with the transfer network system operate under a secure legal and technical regime in order to provide an architecture that supports...
CURRENT ASSIGNEES: INTERCOMPUTER CORP
4
US8380622 | US PATENTS | 19-FEB-2013
19.
Secure electronic payment messaging system with reconcilable finality
A transfer network system for providing communications between commercial buyers and suppliers and their respective banks is provided. Client systems in communication with the transfer network system operate under a secure legal and technical regime in order to provide an architecture that supports...
CURRENT ASSIGNEES: INTERCOMPUTER CORP
4
US20090319422 | US APPLICATIONS | 24-DEC-2009
20.
Secure electronic payment messaging system with reconcilable finality
A transfer network system for providing communications between commercial buyers and suppliers and their respective banks is provided. Client systems in communication with the transfer network system operate under a secure legal and technical regime in order to provide an architecture that supports...
CURRENT ASSIGNEES: INTERCOMPUTER CORP
4
US20050108157 | US APPLICATIONS | 19-MAY-2005

21.
Secure messaging system
A method for secure data transactions over a computer network is described. In one embodiment, the act of generating at the first party a document, which authorizes the data transaction to proceed is performed. In one embodiment, the document content is signed using a computer network with...
CURRENT ASSIGNEES: INTERCOMPUTER CORP
4
US20050257045 | US APPLICATIONS | 17-NOV-2005
22.
Methods for secure cryptogram generation
Embodiments of the invention introduce efficient methods for securely generating a cryptogram by a user device, and validating the cryptogram by a server computer. In some embodiments, a secure communication can be conducted whereby a user device provides a cryptogram without requiring the user...
CURRENT ASSIGNEES: VISA INTL SRVC ASSOC
4
EP3195521B1 | EPO PATENTS | 04-MAR-2020
23.
Methods for secure cryptogram generation
Embodiments of the invention introduce efficient methods for securely generating a cryptogram by a user device, and validating the cryptogram by a server computer. A secure communication can be conducted whereby a user device provides a cryptogram without requiring the user device to persistently...
CURRENT ASSIGNEES: VISA INTL SRVC ASSOC
4
US20190305953 | US APPLICATIONS | 03-OCT-2019
24.
Methods for secure cryptogram generation
Embodiments of the invention introduce efficient methods for securely generating a cryptogram by a user device, and validating the cryptogram by a server computer. In some embodiments, a secure communication can be conducted whereby a user device provides a cryptogram without requiring the user...
CURRENT ASSIGNEES: VISA INTL SRVC ASSOC
4
WO2016033610A1 | WIPO APPLICATIONS | 03-MAR-2016
25.
Methods for secure cryptogram generation
Embodiments of the invention introduce efficient methods for securely generating a cryptogram by a user device, and validating the cryptogram by a server computer. A secure communication can be conducted whereby a user device provides a cryptogram without requiring the user device to persistently...
CURRENT ASSIGNEES: VISA INTL SRVC ASSOC
4
US10389533 | US PATENTS | 20-AUG-2019
26.
Methods for secure cryptogram generation
Embodiments of the invention introduce efficient methods for securely generating a

cryptogram by a user device, and validating the cryptogram by a server computer. In some embodiments, a secure communication can be conducted whereby a user device provides a cryptogram without requiring the user...
CURRENT ASSIGNEES: VISA INTL SRVC ASSOC
4
US20160065370 | US APPLICATIONS | 03-MAR-2016
27.
Electronic device and method for payment transaction
According to various embodiments of the present document, a method of performing a payment transaction in an electronic device and an electronic device includes: receiving payment data generated using authentication information in response to a payment request input through the electronic device,...
CURRENT ASSIGNEES: SAMSUNG ELTNC CO LTD
4
KR20170027160A | KOREA APPLICATIONS | 09-MAR-2017
28.
Methods for secure cryptogram generation
Embodiments of the invention introduce efficient methods for securely generating a cryptogram by a user device, and validating the cryptogram by a server computer. In some embodiments, a secure communication can be conducted whereby a user device provides a cryptogram without requiring the user...
CURRENT ASSIGNEES: VISA INTL SRVC ASSOC
4
US9813245 | US PATENTS | 07-NOV-2017
29.
Methods for secure cryptogram generation
Embodiments of the invention introduce efficient methods for securely generating a cryptogram by a user device, and validating the cryptogram by a server computer. In some embodiments, a secure communication can be conducted whereby a user device provides a cryptogram without requiring the user...
CURRENT ASSIGNEES: VISA INTL SRVC ASSOC
4
EP3195521A1 | EPO APPLICATIONS | 26-JUL-2017
30.
Methods for secure cryptogram generation
Embodiments of the invention introduce efficient methods for securely generating a cryptogram by a user device, and validating the cryptogram by a server computer. A secure communication can be conducted whereby a user device provides a cryptogram without requiring the user device to persistently...
CURRENT ASSIGNEES: LE SAINT ERIC [+2]
4
US20180026787 | US APPLICATIONS | 25-JAN-2018
31.
System and method for secure three-party communications
A system and method for communicating information between a first party and a second party, comprising the steps of receiving, by an intermediary, an identifier of desired information and accounting information for a transaction involving the information from the first party, transmitting an...

CURRENT ASSIGNEES: RPX CORP
4
US8316237 | US PATENTS | 20-NOV-2012
32.
Secure electronic payment messaging system with reconcilable finality
A transfer network system for providing communications (100) between commercial buyers and suppliers and their respective banks (130, 140) is provided. Client systems in communication with the transfer network system operate under a secure legal and technical regime in order to provide an...
CURRENT ASSIGNEES: INTERCOMPUTER CORP
4
WO2004034226A2 | WIPO APPLICATIONS | 22-APR-2004
33.
Systems and methods for reducing fraud risk for a primary transaction account
The system protects an account through the use of tokens, thereby eliminating the need to expose the primary account identifier during a transaction. If a primary account identifier is compromised, any use of the primary account identifier to facilitate a fraudulent purchase or settlement...
CURRENT ASSIGNEES: AMERICAN EXPRESS TRAVEL RELATED SRVC CO INC
4
WO2017180243A1 | WIPO APPLICATIONS | 19-OCT-2017
34.
System and Method For Automated Linkage of Enriched Transaction Data to a Record of Charge
Systems and methods for automated linkage of enriched transaction data to a record of charge are provided. Electronic enriched transaction data, such as receipt information, provided by merchants, merchant aggregators, or third parties may be automatically associated with the corresponding...
CURRENT ASSIGNEES: AMERICAN EXPRESS TRAVEL RELATED SRVC CO INC
4
US20180137506 | US APPLICATIONS | 17-MAY-2018
35.
Secure electronic payment messaging system with reconcilable finality
A transfer network system for providing communications (100) between commercial buyers and suppliers and their respective banks (130, 140) is provided. Client systems in communication with the transfer network system operate under a secure legal and technical regime in order to provide an...
CURRENT ASSIGNEES: INTERCOMPUTER CORP
4
EP1550066A2 | EPO APPLICATIONS | 06-JUL-2005
36.
Systems and methods for automatically securing and validating multi-server electronic communications over a plurality of networks
This disclosure relates to methods and systems for automatically securing and validating multi-server electronic communications over a plurality of networks, without requiring additional physical or programmatic infrastructure on the intermediary servers. A processor-executable component can be...
CURRENT ASSIGNEES: PAY WITH PRIVACY INC

4
WO2017044836A1 | WIPO APPLICATIONS | 16-MAR-2017
37.
Methods for securing transactions by applying crytographic methods to assure mutual identity
Described are a system and method for securing an online transaction. A request is output from an electronic device to a verification server to perform an online transaction. The verification server generates a challenge request. The challenge request is encrypted with a private key of a pair of...
CURRENT ASSIGNEES: ID SECURITY LLC
4
US8601268 | US PATENTS | 03-DEC-2013
38.
Systems and methods for reducing fraud risk for a primary transaction account
The system protects an account through the use of tokens, thereby eliminating the need to expose the primary account identifier during a transaction. If a primary account identifier is compromised, any use of the primary account identifier to facilitate a fraudulent purchase or settlement...
CURRENT ASSIGNEES: AMERICAN EXPRESS TRAVEL RELATED SRVC CO INC
4
US20170300918 | US APPLICATIONS | 19-OCT-2017
39.
Systems and methods for reducing fraud risk for a primary transaction account
The system protects an account through the use of tokens, thereby eliminating the need to expose the primary account identifier during a transaction. If a primary account identifier is compromised, any use of the primary account identifier to facilitate a fraudulent purchase or settlement...
CURRENT ASSIGNEES: AMERICAN EXPRESS TRAVEL RELATED SRVC CO INC
4
EP3443516A1 | EPO APPLICATIONS | 20-FEB-2019
40.
Secure messaging system
A method for secure data transactions over a computer network is described. In one embodiment, the act of generating at the first party a document, which authorizes the data transaction to proceed is performed. In one embodiment, the document content is signed using a computer network with...
CURRENT ASSIGNEES: INTERCOMPUTER CORP
4
WO2005101270A1 | WIPO APPLICATIONS | 27-OCT-2005
41.
Online Security Systems and Methods
Described are a system and method for securing an online transaction. A request is output from an electronic device to a verification server to perform an online transaction. The verification server generates a challenge request. The challenge request is encrypted with a private key of a pair of...
CURRENT ASSIGNEES: ID SECURITY LLC
4
US20120239928 | US APPLICATIONS | 20-SEP-2012

42.
System and method for secure three-party communications
A system and method for communicating information between a first party and a second party, comprising the steps of receiving, by an intermediary, an identifier of desired information and accounting information for a transaction involving the information from the first party, transmitting an...
CURRENT ASSIGNEES: RPX CORP
4
US8904181 | US PATENTS | 02-DEC-2014
43.
Systems and methods for automatically securing and validating multi-server electronic communications over a plurality of networks
This disclosure relates to methods and systems for automatically securing and validating multi-server electronic communications over a plurality of networks, without requiring additional physical or programmatic infrastructure on the intermediary servers. A processor-executable component can be...
CURRENT ASSIGNEES: PAY WITH PRIVACY INC
4
US20170070484 | US APPLICATIONS | 09-MAR-2017
44.
Secure messaging system
A method for secure data transactions over a computer network is described. In one embodiment, the act of generating at the first party a document, which authorizes the data transaction to proceed is performed. In one embodiment, the document content is signed using a computer network with...
CURRENT ASSIGNEES: INTERCOMPUTER CORP
4
EP1738239A1 | EPO APPLICATIONS | 03-JAN-2007
45.
Techniques for optimizing communication protocols
A thin client may be utilized to facilitate data exchanges between two devices (e.g., a remote computer and a portable device). In some embodiments, the two devices may utilize differing communications protocols. The thin client may further be configured with a rules engine that determines one or...
CURRENT ASSIGNEES: VISA INTL SRVC ASSOC
4
WO2019177990A1 | WIPO APPLICATIONS | 19-SEP-2019
46.
Secure authentication system and method
Methods and systems pertaining secure transaction systems are disclosed. In one implementation, a merchant server payment information from a user computer. The merchant server can transmit a verification request to a gateway as well as receive a verification response from the gateway. The merchant...
CURRENT ASSIGNEES: VISA INTL SRVC ASSOC
4
US20180308095 | US APPLICATIONS | 25-OCT-2018
47.
System, method and storage medium for secure password generation

Embodiments of the present invention introduce an efficient method for securely generating a password by a user device and verifying the password by a server computer. In some embodiments, secure communications may be performed by way of a user device providing a password without requiring the user...
CURRENT ASSIGNEES: VISA INTL SRVC ASSOC
4
CN106797311B | CHINA PATENTS | 14-JUL-2020
48.
System and method for electronic payment
A system and method for conducting electronic payment transactions between transaction initiators and transaction responders is disclosed. The system comprises a server system in communication with transactional infrastructure of the transaction initiators and transaction responders and enables a...
CURRENT ASSIGNEES: JEREMIAH 33 FAMILY TRUST [+1]
4
US20170255908 | US APPLICATIONS | 07-SEP-2017
49.
Apparatus and Methods for Providing Scalable, Dynamic, Individualized Credential Services Using Mobile Telephones
Apparatus and methods perform transactions in a secure environment between an individual and another party, such as a merchant, in various embodiments. The individual possesses a mobile electronic device, such as a smartphone, that can encrypt data according to a public key infrastructure. The...
CURRENT ASSIGNEES: SURIDX INC
4
US20090132813 | US APPLICATIONS | 21-MAY-2009
50.
Social Data Tracking Datastructures, Apparatuses, Methods and Systems
The Social Data Tracking Datastructures, Apparatuses, Methods and Systems (“SDTD”) transforms brokerage order request, blockchain transaction request, agency action request inputs via SDTD components into brokerage order confirmation, transaction confirmation, agency action notification outputs. An...
CURRENT ASSIGNEES: FMR LLC
4
US20190188699 | US APPLICATIONS | 20-JUN-2019

Google

adding the smart contract into the blockchain

All | News | Videos | Images | Shopping | More | Settings | Tools

Jan 1, 2000 – Aug 14, 2015 | All results | Clear

Ad · www.apttus.com/smart-contract/platform

How Do Smart Contracts Work? - Prepare Your Career & Company

Free Guide to Streamlining Your Business with **Smart Contracts**, **Blockchain**, & AI. Enhance Your **Smart Contract** Platform. Simplify Audits. Reduce Risk. Speed Cycle Times. Cut Costs. Services: Accounting Management, Revenue Management, Billing Management.

Ad · executive-education-online.mit.edu/mit-blockchain/online-course · (617) 539-8980

MIT Online Blockchain Course - Learn Blockchain Technology

Explore the Business Innovation of **Blockchain** Technologies in 6 Weeks Online. Apply Now. Discover the Possibilities and Limitations of **Blockchain** in this Online Course from MIT. Online Short Course. Flexible Learning. Weekly Modules. Structured Approach.

Ad · www.fairfood.nl/free-report

Blockchain for smallholders - Blockchain for beginners

A chain of possibilities: **blockchain** for agrifood report by Fairfood & wageningen. **Blockchain** for supply chain finance, farmer inclusion & supply chain transparency. Download Report. View Solutions. View Resources.
Our Solutions · Contact Form · Blog Center · About Us

Ad · www.slovakstartup.com/

Biotron Blockchain Solution - Read The Interview with CEO

Background info about new personal data solution on **blockchain** from Slovakia. View News View Guest & Experts. Highlights. A Startup Media Platform, Magazine Available.

www.iit.cnr.it › sites › default › files › blockchain-base... · PDF

Blockchain Based Access Control Services - IIT - CNR

Jan 15, 2013 - resented as a **smart contract** which is stored on the **blockchain** through ... be **added to the blockchain**. inserting into the **smart contract** a function call to retrieve.
by DDF Maesa - Cited by 11 - Related articles

www.fastcompany.com › smart-contracts-could-be-cry...

What Are Smart Contracts? Cryptocurrency's Killer App

Sep 17, 2014 - **Smart contracts** are really the killer app of the **cryptocurrency** world. ... Because **smart contracts** are computer programs, it would be trivial to add more complex ...

iang.org › papers › intersection_ricardian_smart

On the intersection of Ricardian and Smart Contracts - Iang

Feb 2, 2015 - Bitcoin's inclusion of the **smart contract** form invented by Nick Szabo has thrust ... who can insert the entire code into the mediating agent (**blockchain** or at least ...

blog.ethereum.org › 2015/08/07 › on-public-and-priva...

On Public and Private Blockchains | Ethereum Foundation Blog

Aug 7, 2015 - To summarize, there are generally three categories of **blockchain**-like ... for determining what blocks get **added** to the chain and what the current state is. ... Note that by creating privately administered **smart contracts** on public **blockchains**, ...

www.healthit.gov › sites › default › files › 12-55-block... · PDF

A Blockchain-Based Approach to Health Information ...

Aug 19, 2012 - Miners are nodes that assemble the blocks and **add** them **to the blockchain**. ... with our healthcare use case, **smart contracts** will play an important role.
by K Peterson - Cited by 155 - Related articles

arxiv.org › pdf ▾ PDF

Blockchain Technology as a Regulatory Technology - arXiv

Sep 15, 2014 - blockchain technology and associated smart contracts, code is assuming an even stronger role in ... than 50% of the network nodes) by adding new data to it.
by P De Filippi - 2018 - Cited by 115 - Related articles

www.coindesk.com › new-blockchain-startup-brings-co... ▾

New Blockchain Startup Brings Contracts into the Digital Age

Dec 10, 2014 - SmartContract is harnessing blockchain technology to create customisable ... who added that a four-person team was assembled to develop the SmartContract ...

isg-one.com › consulting › blockchain › articles › can-... ▾

Can Blockchain Improve Network Management? - ISG

Apr 1, 2011 - ... to smart contracts (business rules configured into the blockchain). The added benefit of this approach is recording change management approvals directly into ...

eprints.lancs.ac.uk › eprint › IOTSMS_2018_paper_28 ▾ PDF

use style: paper title - Lancaster EPrints - Lancaster University

Jan 15, 2010 - blockchain technology to its full potential. With the addition of smart contracts and Ethereum VM, the capacity of. Ethereum had immensely increased. Of the many ...
by J Joseph - 2019 - Cited by 3 - Related articles

ieeexplore.ieee.org › document

Legally Speaking: Smart Contracts, Archival Bonds, and ...

Oct 15, 2011 - Abstract: As currently understood and used, "smart contracts" are merely a ... This paper, however, proposes the creation of a semantic legal layer to support blockchain based legal contracts. ... Date Added to IEEE Xplore: 18 September 2017.
by DL Hofman - 2017 - Cited by 7 - Related articles

Ad · www.jpmorgan.com/ ▾

J.P. Morgan - The Future of Blockchain

Leading blockchain technology to actively develop in-house solutions. Aiming to actualize enterprise-grade blockchain tools, such as JPM Coin, IIN ® and Quorum®.
IIN® · Next Step for Blockchain · JPM Coin for Payments · Quorum® · Dromaius

Ad · www.simbachain.com/ ▾

Build Blockchain Apps - No Coding Required

SIMBA Chain let's anyone build Blockchain apps regardless of programming experience. Chat Support Available. View Pricing. Download E-Book. Sign Up Online. Steps: Choose Your Network, Choose Your File Storage, Create A Smart Contract, Deploy.
Pricing Information · Watch Demo · Online Resources · Platform Services

Ad · www.coingeek.com/bitcoin101/smart-contracts ▾

Explained - What is a smart contract?

In this guide we look at what Smart Contracts are and how can they be used on BSV. What are the use cases of Smart Contracts and how to start using them. Subscribe To Events. View Our Guides.
CoinGeek Conversations · Latest News

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	1	"20180247302".did.	US-PGPUB; USPAT	OR	ON	2020/09/10 18:26
S2	8	("2018/0247302").URPN.	USPAT	OR	ON	2020/09/10 18:27
S3	8	("2018/0247302").URPN.	USPAT	OR	ON	2020/09/14 17:18
S4	8	("2018/0247302").URPN.	USPAT	OR	ON	2020/09/14 17:19
S5	0	"20200143476".did.	USPAT	OR	ON	2020/09/14 17:26
S6	1	"20200143476".did.	US-PGPUB; USPAT	OR	ON	2020/09/14 17:27
S7	1	"20160342994".did.	US-PGPUB; USPAT	OR	ON	2020/09/17 15:59
S8	59	("2016/0342994").URPN.	USPAT	OR	ON	2020/09/17 15:59
S9	59	("2016/0342994").URPN.	USPAT	OR	ON	2020/09/17 16:00
S10	39	S8 and "smart contract"	USPAT	OR	ON	2020/09/17 16:01
S11	24	S10 and @ad<"20160812"	USPAT	OR	ON	2020/09/17 16:01
S12	59	("2016/0342994").URPN.	USPAT	OR	ON	2020/09/17 18:23
S13	39	S12 and "smart contract"	USPAT	OR	ON	2020/09/17 18:23
S14	5	S13 and @ad<"20150814"	USPAT	OR	ON	2020/09/17 18:23
S15	24	S13 and @ad<"20160812"	USPAT	OR	ON	2020/09/17 18:30
S16	19	S15 not S14	USPAT	OR	ON	2020/09/17 18:30
S17	116	("20030126094" | "20040172535" | "20040199463" | "20050256802" | "20080301043" | "20090281948" | "20100279653" | "20110078073" | "20110197064" | "20120066121" | "20120284175" | "20130198061" | "20130232056" | "20130311375" |	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/17 18:34

		"20140006185" | "20140040114" | "20140089243" | "20140310171" | "20150052587" | "20150172053" | "20150206106" | "20150262137" | "20150332283" | "20150379510" | "20150379636" | "20160012424" | "20160028552" | "20160050203" | "20160092874" | "20160125376" | "20160125414" | "20160191243" | "20160275461" | "20160292672" | "20160321654" | "20160323109" | "20160342978" | "20160342989" | "20160342994" | "20170005804" | "20170011460" | "20170041296" | "20170046526" | "20170046651" | "20170046664" | "20170046680" | "20170046806" | "20170091397" | "20170103167" | "20170103461" | "20170109735" | "20170116693" | "20170132625" | "20170132626" | "20170132630" | "20170140375" | "20170163733" | "20170177855" | "20170178131" | "20170178237" | "20170180134" | "20170200137" | "20170213209" | "20170214675" | "20170214698" | "20170220998" | "20170221052" | "20170223005" | "20170228447" | "20170228822" | "20170230378" | "20170232300" | "20170235955" | "20170236407" | "20170243020" | "20180053161" | "20180268479" | "5671283" | "5835599" | "6073234" | "6324286" | "6725303" | "6850252" | "6973187" | "7055039" | "7092400" | "7184549" | "7362859" | "7392384" | "7428306" | "7502933" | "7574401" | "7649992" | "7764788" | "7979889" | "8078874" | "8107621" | "8155311" | "8259934").PN. OR ("8358781" | "8396209" | "8397841" | "8416947" | "8458461" | "8464320" | "8516266" | "8590055" | "8737606" | "8942374" | "8983063" | "9059866" | "9083702" | "9092766" | "9298806" | "9635000" | "9672499").PN.				
S18	20	S17 and "smart contract"	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/17 18:36
S19	0	S18 and @ad<"20150814"	USPAT	OR	ON	2020/09/17 19:49

S20	50	("20030009413" | "20030225672" | "20080140578" | "20100228674" | "20100250447" | "20110231913" | "20130061049" | "20130238478" | "20130238903" | "20130254052" | "20140280476" | "20140344015" | "20150120567" | "20150170112" | "20150227897" | "20150244690" | "20150262137" | "20150262173" | "20150269557" | "20150310424" | "20150324787" | "20150332283" | "20150356523" | "20150356555" | "20150363777" | "20150363783" | "20150379510" | "20160027229" | "20160028552" | "20160078219" | "20160080156" | "20160112200" | "20160125040" | "20160261404" | "20160342994" | "7356696" | "7359877" | "7487123" | "7778915" | "7895112" | "7921051" | "7933827" | "7974907" | "8132005" | "8190893" | "8244622" | "8386362" | "8412952" | "8606685" | "9298806").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/17 19:51
S21	15	S20 and @ad<"20150814"	USPAT	OR	ON	2020/09/17 19:52
S22	0	S21 and "smart contract"	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/17 19:56
S23	8	("2018/0247302").URPN.	USPAT	OR	ON	2020/09/17 19:59
S24	12	("20170017955" | "20170048209" | "20170109735" | "20170132630" | "20170221029" | "20170221052" | "20170232300" | "20170337534" | "20170352012" | "20180096752" | "20180247302" | "20180337769").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/17 20:00
S25	0	S24 and @ad<"20150814"	USPAT	OR	ON	2020/09/17 20:02
S26	120	("20030126094" | "20040172535" | "20050256802" | "20060053296" | "20090281948" | "20100279653" | "20110078073" | "20110197064" | "20120066121" | "20120284175" | "20130198061" | "20130232056" | "20130311375" | "20140006185" | "20140089243" | "20140310171" | "20150052587" | "20150172053" | "20150206106" | "20150242605" | "20150254446" | "20150332283" | "20150379510" | "20150379636" |	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/17 20:03

		"20160012424" | "20160028552" | "20160035054" | "20160050203" | "20160092874" | "20160125376" | "20160125414" | "20160140562" | "20160191243" | "20160275461" | "20160292672" | "20160321654" | "20160323109" | "20160342978" | "20160342989" | "20160342994" | "20160379211" | "20170005804" | "20170011460" | "20170046526" | "20170046651" | "20170046664" | "20170046680" | "20170054611" | "20170091397" | "20170103167" | "20170103461" | "20170116693" | "20170132625" | "20170132626" | "20170132630" | "20170140375" | "20170140394" | "20170163733" | "20170177855" | "20170178131" | "20170178237" | "20170180134" | "20170200137" | "20170213209" | "20170214675" | "20170214698" | "20170220998" | "20170221052" | "20170223005" | "20170228447" | "20170230378" | "20170232300" | "20170235955" | "20170236407" | "20170243020" | "20170243208" | "20170243213" | "20170339125" | "5671283" | "5835599" | "6073234" | "6324286" | "6725303" | "6850252" | "6973187" | "7055039" | "7092400" | "7184549" | "7362859" | "7392384" | "7428306" | "7502933" | "7574401" | "7649992" | "7764788" | "7979889" | "8078874" | "8107621" | "8155311").PN. OR ("8259934" | "8302153" | "8358781" | "8396209" | "8397841" | "8416947" | "8458461" | "8464320" | "8516266" | "8590055" | "8737606" | "8942374" | "8983063" | "9059866" | "9083702" | "9092766" | "9298806" | "9319469" | "9635000" | "9672499" | "9805213").PN.				
S27	40	S26 and @ad<"20150814"	USPAT	OR	ON	2020/09/17 20:03
S28	0	S27 and "smart contract"	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/17 20:03
S29	88	((financial, payment) adj transaction) with ((data, information) and (blockchanin, "block chain"))	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/18 10:12

S30	15	S29 and @ad<"20150814"	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/18 10:13
S31	1	"20200143476".did.	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/18 12:22
S32	0	("2020/0143476").URPN.	USPAT	OR	ON	2020/09/18 12:22
S33	1,359	((financial, payment) adj transaction) and (blockchanin, "block chain")	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/18 12:30
S34	1,606	((financial, payment) adj transaction) and (blockchanin, "block chain")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/09/18 12:30
S35	1,437	((financial, payment) adj transaction) and (blockchanin, "block chain")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; IBM_TDB	OR	ON	2020/09/18 12:31
S36	103	S35 and @ad<"20150814"	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/18 12:33
S37	54	S36 and token	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/18 12:33
S38	8	("2018/0247302").URPN.	USPAT	OR	ON	2020/09/21 18:11
S39	12	("20170017955" | "20170048209" | "20170109735" | "20170132630" | "20170221029" | "20170221052" | "20170232300" | "20170337534" | "20170352012" | "20180096752" | "20180247302" | "20180337769").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/21 18:12
S40	1	S39 and @ad<"20150814"	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/21 18:19
S41	1	"20170005804".did.	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/21 18:23
S42	1	"20160292672".did.	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/21 18:24

S43	1	"20150379510".did.	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/21 18:53
S44	1	"20170132630".did.	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/21 18:55
S45	1	"9967334".pn.	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/21 18:55
S46	70	("20010049726" | "20020143819" | "20050004804" | "20060069647" | "20060100955" | "20080320565" | "20090150972" | "20120163584" | "20130329883" | "20140201057" | "20140279433" | "20140344015" | "20150006739" | "20150228004" | "20150287026" | "20150310424" | "20150348017" | "20150356524" | "20150356555" | "20150371224" | "20150379510" | "20160071108" | "20160086175" | "20160162882" | "20160217436" | "20160218879" | "20160254910" | "20160260069" | "20160260169" | "20160267472" | "20160275461" | "20160283920" | "20160292672" | "20160300227" | "20160300234" | "20160306966" | "20160321654" | "20160330027" | "20160330031" | "20160335628" | "20160342977" | "20160342978" | "20160342989" | "20160342994" | "20160344543" | "20160350749" | "20160358184" | "20170005804" | "20170061398" | "20170236123" | "20170243241" | "20170279800" | "20170295021" | "20170310653" | "6591292" | "7130999" | "7293270" | "8886570" | "9135787" | "9256467" | "9298806" | "9397985" | "9406063" | "9514293").PN. OR ("9967334").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/21 18:56
S47	40	S46 and @AD<"20150814"	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/21 18:57
S48	1	"20170255908".did.	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/21 21:29
S49	3	("2017/0255908").URPN.	USPAT	OR	ON	2020/09/21 21:30

S50	79	("10311413" | "20010056390" | "20020123949" | "20040015392" | "20040081302" | "20050160035" | "20050177448" | "20060089877" | "20060229984" | "20070233615" | "20070244811" | "20070255653" | "20070255662" | "20080052176" | "20080275779" | "20080275811" | "20090119171" | "20090119190" | "20090171839" | "20090177497" | "20090288012" | "20100017324" | "20100078472" | "20100088207" | "20100100480" | "20100121745" | "20100174644" | "20100205091" | "20110125643" | "20110166883" | "20110246342" | "20110251952" | "20120150706" | "20120166332" | "20120197788" | "20120259688" | "20120259779" | "20130013506" | "20130132244" | "20130227353" | "20130290177" | "20130297486" | "20130311362" | "20130346302" | "20140070001" | "20140081854" | "20140114842" | "20140180929" | "20140244477" | "20140279098" | "20140351118" | "20150142657" | "20150220904" | "20150364017" | "20160005037" | "20160071094" | "20160253731" | "20170004463" | "20170004467" | "20170004468" | "20170255908" | "5699528" | "5943656" | "6636833" | "6757371" | "7136835" | "7577610" | "7958049" | "8417628" | "8533079" | "8595134" | "8630949" | "8688552" | "8732044" | "8744965" | "8751384" | "8793184" | "8799157" | "9824342").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/21 21:30
S51	77	S50 and @ad<"20150814"	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/21 21:31
S52	0	S51 and ("block-chain", "block chain")	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/21 21:32
S53	0	S51 and "smart contract"	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/21 21:33
S54	68	S51 and transaction	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/21 21:33

S55	17	S54 and token	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/21 21:33
S56	1	"20140108260".did.	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/21 21:37
S57	32	("2014/0108260").URPN.	USPAT	OR	ON	2020/09/21 21:38
S58	9	S57 and @ad<"20150814"	USPAT	OR	ON	2020/09/21 21:38
S59	170	(financial adj transaction) and (block-chain, blockchain, "block chain") same "smart contract"	USPAT	OR	ON	2020/09/21 22:22
S60	0	S59 and @AD<"20150415"	USPAT	OR	ON	2020/09/21 22:23
S61	1	S59 and @AD<"20150814"	USPAT	OR	ON	2020/09/21 22:24
S62	15	("20070055552" | "20090076855" | "20090144200" | "20140344015" | "20140368601" | "20140372140" | "20150244690" | "7356696" | "7600255" | "8412952" | "8615532").PN. OR ("10340038").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/21 22:25
S63	11	S62 and @ad<"20150814"	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/21 22:26
S64	614	(financial near2 transaction) and (block-chain, blockchain, "block chain")	USPAT	OR	ON	2020/09/21 22:33
S65	53	S64 and @ad<"20150814"	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/21 22:34
S66	25	S65 and token	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/21 22:35
S67	28	S65 not S66	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/21 22:36
S68	62	("20100306032" | "20130282580").PN. OR ("9298806").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/21 22:41
S69	7	S68 and @ad<"20150814"	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/21 22:41
S70	1	"20170244757".did.	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/21 23:02

S71	17	("2017/0244757").URPN.	USPAT	OR	ON	2020/09/21 23:03
S72	0	S71 and @ad<"20150814"	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/21 23:03

9/22/2020 6:09:22 PM
C:\Users\aabdullaev\Documents\EAST\Workspaces\15752711.wsp

Google

financial transaction via smart contract

All | News | Images | Videos | Shopping | More | Settings | Tools

Jan 1, 2000 – Aug 14, 2015 | All results | Clear

www.fastcompany.com › smart-contracts-could-be-cry...

What Are Smart Contracts? Cryptocurrency's Killer App

Sep 17, 2014 - **Smart contracts** are computer programs that can automatically execute the terms of a contract. Someday, these programs may replace lawyers and banks for handling certain common **financial transactions**. And the potential for **smart contracts** goes way beyond simple transfers of funds.

People also ask

- How much does it cost to deploy a smart contract?
- How do smart contracts work?
- Is a smart contract a contract?
- Can smart contracts be hacked?

Feedback

ieet.org › index.php › IEET2 › more › swan20150223

Top 5 Immediate Money-Making Applications of Blockchain ...

Feb 23, 2015 - In financial markets, one clear application of blockchain technology is algorithmic ... Blockchains instantiate a robust technology record of all transactions in a ... like the mortgage industry could implement smart property via blockchains as a ... In the same vein as **smart contract**-based algorithmic trading, blockchains are also ...

www.gibsondunn.com › documents › publications › Le... PDF

Blockchain Technology and Legal Implications of - Gibson Dunn

Mar 31, 2015 - and "smart" **contracts** can be built. ... rencies in financial **transactions**.5 With Crypto 2.06 and ... verified via a blockchain ledger, and the resulting veri-.

by JA LEE - 2015 - Cited by 5 - Related articles

isg-one.com › consulting › blockchain › articles › smar...

Smart Contracts: The Future of Contracting - ISG

Apr 1, 2011 - For a **transaction** on a blockchain network to take place, a **smart contract** ensures ... by a **smart contract** and the **transaction** is often completed via the exchange of . understanding of finance, sales and marketing along with communication and ...

fc16.ifca.ai › bitcoin › papers › DAKMS16 PDF

Step by Step Towards Creating a Safe Smart Contract ...

Jan 15, 2014 - contracts, **smart contracts** carry the promise of low legal and **transaction** costs, ... terparties may attempt to cheat in arbitrary ways that maximize their economic gains ... walk the student through the typical pitfalls in programming safe smart con-

by K Delmolino - Cited by 413 - Related articles

www.wired.com › insights › 2015/01 › block-chain-2-0

Block Chain 2.0: The Renaissance of Money | WIRED

Jan 6, 2015 - Apart from **Financial transactions**, **smart contracts** are now entering the Legal ... Another way to look at it is that smart property can be controlled via the Block ...

s3-us-west-2.amazonaws.com › chainbook › Great+Chain... PDF

Smart Contracts - Amazon S3 - AWS

Feb 24, 2014 - Smart property is property whose ownership is controlled via **smart contracts** that ... platform, computing infrastructure, **transaction** platform and **financial** services ...

arxiv.org › pdf PDF

Cryptographically-secure Off-chain Multi-asset Instant ... - arXiv

Jan 15, 2009 - COMIT is a super blockchain network that allows for instant **transactions** which are enforced using off-chain smart ... **financial** business logic via **smart contracts**.
by D Hosp - 2018 - Cited by 7 - Related articles

arxiv.org › pdf PDF

Blockchain Technology as a Regulatory Technology - arXiv

Sep 15, 2014 - blockchain technology and associated **smart contracts**, code is assuming an ... knowledge domains (such as health care and tax or **financial** regulations) for automated or semi- ... trustless **transactions** via integrated enforcement mechanisms.
by P De Filippi - 2018 - Cited by 115 - Related articles

www.sciencedirect.com › science › article › pii

A smart contract system for security of payment of construction ...

Feb 4, 2012 - In this paper a novel **smart contract** payment security system named SMTSEC is ... The progress payments are in general made **through** a cascade system; the ... presented **smart contract** functions for **financial transactions** and examined the ...

Ad · www.apttus.com/smart-contract/platform

How Do Smart Contracts Work? - Prepare Your Career & Company

Free Guide to Streamlining Your Business with **Smart Contracts**, Blockchain, & AI. Enhance Your **Smart Contract** Platform. Reduce Risk. Simplify Audits. Cut Costs. Speed Cycle Times. Services: Accounting Management, Revenue Management, Billing Management.
Ready for Smart Contracts · How Legal Uses Applied AI · Regulatory Compliance

Ad · www.fabriik.com/

Fabriik Digital Asset Creator - Smart Contracts on BSV

Fabriik is the only BSV Token Creator that doesn't require any coding ability. The possibilities are endless when you can Create **Smart Contracts** on BitcoinSV. **Smart Contracts** and DAPPs. Apply Online. No Coding Needed. Create Digital Assets.

Ad · search.walletgenius.com/financial/info

Financial Agreement Contract - Financial Agreement Contract

Search **Financial** agreement **contract** at WalletGenius. Look Up Results On Walletgenius Find & Compare Your Options To Find The Best Price For You. Filing Taxes. Asset Management Services. Account Information. Budgeting Services.
Identity Protection · Refinance Mortgage · Identity Theft Protection · Refinance Rates

Charlottesville VA, Virginia - Based on your past activity - Use precise location - Learn more

Help Send feedback Privacy Terms

About 185 results

Download with Concepts Side-by-si

Sort by · Relevance · Group by · None · Deduplicate by · Family · Results / page · 10

Point-to-point transaction guidance apparatuses, methods and systems



US · US10339522B2 · John C. McConnaughey · Fmr Llc

Priority 2015-07-14 · Filed 2016-07-13 · Granted 2019-07-02 · Published 2019-07-02

... the SOCOACT Server 5801 including client portfolio data, **financial transaction** data, and any other data as described, contemplated and used herein. ... , for example, the Fed may issues funds on the **blockchain**. Upon creating a 'trust' between counterparts with special encrypted **token/smart contracts**.

Computationally efficient transfer processing, auditing and searching apparatus ...



WO EP CN JP CA · JP2018525728A · [illegible]

Priority 2015-07-14 · Filed 2016-07-13 · Published 2018-09-06

The network environment 100 can further include a SOCOACT database 5819, including client portfolio data, **financial transaction** data and other data ... When creating a "trust" between parties with special cryptographic **tokens** / **smart contracts**, the financial institution creates a permitted **blockchain** ...

Social Aggregating, Fractionally Efficient Transfer Guidance, Conditional ...



US · US20170048234A1 · Timothy Lohe · Fmr Llc

Priority 2015-07-14 · Filed 2016-07-14 · Published 2017-02-16

... the SOCOACT Server 5801 including client portfolio data, **financial transaction** data, and any other data as described, contemplated and used herein. ... **smart contract** fulfillment component means, to: obtain, via at least one processor, a first encrypted **token** for the **crypto** 2-party transaction ...

Smart Rules and Social Aggregating, Fractionally Efficient Transfer Guidance, ...



US · US20170085545A1 · Timothy Lohe · Fmr Llc

Priority 2015-07-14 · Filed 2016-07-14 · Published 2017-03-23

... the SOCOACT Server 5801 including client portfolio data, **financial transaction** data, and any other data as described, contemplated and used herein. ... , for example, the Fed may issues funds on the **blockchain**. Upon creating a 'trust' between counterparts with special encrypted **token/smart contracts**.

Crypto Captcha and Social Aggregating, Fractionally Efficient Transfer Guidance ...



US · US20170048235A1 · Timothy Lohe · Fmr Llc

Priority 2015-07-14 · Filed 2016-07-14 · Published 2017-02-16

... the SOCOACT Server 5801 including client portfolio data, **financial transaction** data, and any other data as described, contemplated and used herein. ... , for example, the Fed may issues funds on the **blockchain**. Upon creating a 'trust' between counterparts with special encrypted **token/smart contracts**.

Asynchronous **Crypto** Asset Transfer and Social Aggregating, Fractionally ...



US · US20180191503A1 · Vijaya Subhash Alwar · Fmr Llc

Priority 2015-07-14 · Filed 2018-02-15 · Published 2018-07-05

... the SOCOACT Server 7901 including client portfolio data, **financial transaction** data, and any other data as described, contemplated and used herein. ... , for example, the Fed may issues funds on the **blockchain**. Upon creating a 'trust' between counterparts with special encrypted **token/smart contracts**.

Point-to-Point Transaction Guidance Apparatuses, Methods and Systems



US · US20170085555A1 · Dmitry Bisikalo · Fmr Llc

Priority 2015-07-14 · Filed 2016-07-13 · Published 2017-03-23

... the SOCOACT Server 5801 including client portfolio data, **financial transaction** data, and any other data as described, contemplated and used herein. ... , for example, the Fed may issues funds on the **blockchain**. Upon creating a 'trust' between counterparts with special encrypted **token/smart contracts**.

Crypto Key Recovery and Social Aggregating, Fractionally Efficient Transfer ...



US · US20170048209A1 · Timothy Lohe · Fmr Llc

Priority 2015-07-14 · Filed 2016-07-14 · Published 2017-02-16

... the SOCOACT Server 5801 including client portfolio data, **financial transaction** data, and any other data as described, contemplated and used herein. ... , for example, the Fed may issues funds on the **blockchain**. Upon creating a 'trust' between counterparts with special encrypted **token/smart contracts**.

Point-to-Point Transaction Guidance Apparatuses, Methods and Systems



US · US20170091756A1 · Hadley Roger Stern · Fmr Llc

Priority 2015-07-14 · Filed 2016-07-13 · Published 2017-03-30

... the SOCOACT Server 5801 including client portfolio data, **financial transaction** data, and any other data as described, contemplated and used herein. ... , for example, the Fed may issues funds on the **blockchain**. Upon creating a 'trust' between counterparts with special encrypted **token/smart contracts**.

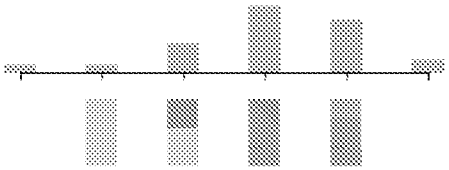
Crypto Voting and Social Aggregating, Fractionally Efficient Transfer Guidance, ...



US • [redacted] • Timothy Lohe • Fmr Llc
Priority 2015-07-14 • Filed 2016-07-14 • Published 2017-02-16
... the SOCOACT Server 5801 including client portfolio data, **financial transaction** data, and any other data as described, contemplated and used herein. ... **blockchain** datastructure. 4 . The apparatus of claim 3 , wherein the user satisfies the **smart contract** by transferring a **crypto token** from a **crypto** ...

Next › » About 185 results

Top 1000 results by filing date



Relative count of top 5 values

Assignees	Inventors	CPCs
Fmr Llc		8.1%
402 Technologies S.A.		3.2%
安全第一公司		3.2%
Security First Corp.		2.7%
Eagency, Inc.		2.7%

Expand

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 15/752,711	Filing Date 02/14/2018	☐ To be Mailed

ENTITY: ☐ LARGE ☑ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*		x $50 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $230 =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT	04/21/2020	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 20	Minus	** 20	= 0		x $50 =	0
	Independent (37 CFR 1.16(h))	* 3	Minus	*** 3	= 0		x $230 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	0

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=		x $0 =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=		x $0 =	
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.	LIE
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	/SHARON D HARRIS/
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".	
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.	

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	Atty. Ref.: AMK-5243-0009
ARMSTRONG et al.	Confirmation No. 5327
Appl. No. 15/752,711	Art Unit: 3691
Filed: 02/14/2018	Examiner: MARSH, JORDAN W

For: COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR

* * * * * * * * * * *

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

April 21, 2020

Sir:

AMENDMENT

In response to the Office Action dated October 21, 2019, the period for response having been extended three (3) month(s) by petition herewith, please amend the above-identified patent application as follows:

Amendments to the Claims are reflected in the listing of claims which begins on page 2.

Remarks/Arguments begin on page 8.

AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1-58. (Canceled)

59. (Currently Amended) A computer implemented method for processing a financial transaction, the method comprising the steps of:

transmitting one or more documents pertaining to the financial transaction, from a first intermediary server in a centralised financial system to a first document store;

generating an enriched data record from the one or more documents, at the first intermediary server, and adding the enriched data record into a blockchain being a distributed ledger, from the first intermediary ~~sever~~server;

requesting generation of a token corresponding to the financial transaction to identify the one or more documents, to a token server, from the first intermediary server, via a messaging bus in the centralised financial system;

generating the token at the token server and adding the token into the blockchain from the token server in association with the enriched data record;

transmitting the token to the first intermediary server from the token server, via the messaging bus; and

transmitting the token from the first intermediary server to the first document store in association with the one or more documents.

60. (Previously Presented) The computer implemented method as claimed in claim 59, further comprising the step of sending a first financial message comprising the token, from the first intermediary server to a second intermediary server in the centralised financial system, indicative of making a payment to a second user.

61. (Previously Presented) The computer implemented method as claimed in claim 59, further comprising the steps of:

implementing a smart contract at the token server; and

adding the smart contract into the blockchain, from the token server.

62. (Currently Amended) The computer implemented method as claimed in claim 59, further comprising the steps of:

transmitting the token from the first intermediary server to a first digital device available with a first user;

providing the token to a second user, by the first user;

providing the token to a second intermediary server in the centralised financial system, from ~~the~~a second digital device;

transmitting the token to a second document store, from the second intermediary server; and

sending a second financial message comprising the token, from the second intermediary server to the first intermediary server, indicative of making a payment to the first user.

63. (Previously Presented) The computer implemented method as claimed in claim 59, wherein the step of generating the enriched data record comprises:

extracting a plurality of attributes from the one or more documents, at the first intermediary server; and

combining the plurality of attributes to generate the enriched data record, at the first intermediary server.

64. (Previously Presented) The computer implemented method as claimed in claim 59, wherein the step of generating the enriched data record comprises:

extracting a plurality of attributes from the one or more documents, at the first intermediary server;

de-identifying the plurality of attributes to obtain a plurality of de-identified attributes, at the first intermediary server; and

combining the plurality of de-identified attributes to generate the enriched data record, at the first intermediary server.

65. (Previously Presented) The computer implemented method as claimed in claim 59, wherein the step of generating the enriched data record comprises:

extracting a plurality of attributes from the one or more documents, at the first intermediary server;

hashing the plurality of attributes to generate a plurality of respective hashes, at the first intermediary server; and

combining the plurality of hashes to generate the enriched data record, at the first intermediary server.

66. (Previously Presented) The computer implemented method as claimed in claim 59, further comprising the steps of:

transmitting one or more first requests, each comprising the token, from the first intermediary server to a second intermediary server in the centralised financial system, via the messaging bus;

receiving the one or more first requests at the second intermediary server and transmitting the one or more first requests and the token from the second intermediary server to a second document store;

generating one or more first responses, each comprising the token, corresponding to the respective one or more first requests, at the second intermediary server;

transmitting the one or more first responses from the second intermediary server to the first intermediary server, via the messaging bus;

hashing the one or more first requests and the one or more first responses at the second intermediary server to generate one or more first request hashes and one or more first response hashes, respectively;

adding the one or more first request hashes and the one or more first response hashes to the enriched data record in the blockchain, from the second intermediary server; and

receiving the one or more first responses at the first intermediary server and transmitting the one or more first responses to the first document store.

67. (Previously Presented) The computer implemented method as claimed in claim 66, further comprising the steps of:

hashing the one or more first responses at the first intermediary server to regenerate the one or more first response hashes; and

verifying the one or more first response hashes with the blockchain from the first intermediary server, using the token.

68. (Previously Presented) The computer implemented method as claimed in claim 66, wherein each one of the one or more first requests are:

encrypted with a second public key and signed with a first public key at the first intermediary server, before transmission to the second intermediary server; and

decrypted with a second private key at the second intermediary server after reception from the first intermediary server; and

wherein each one of the one or more first responses are:

encrypted with the first public key and signed with the second public key at the second intermediary server, before transmission to the first intermediary server; and

decrypted with a first private key at the first intermediary server after reception from the second intermediary server.

69. (Previously Presented) The computer implemented method as claimed in claim 59, further comprising the steps of:

transmitting one or more second requests, each comprising the token, from a second intermediary server in the centralised financial system to the first intermediary server, via the messaging bus;

receiving the one or more second requests at the first intermediary server and transmitting the one or more second requests from the first intermediary server to the first document store;

generating one or more second responses, each comprising the token, corresponding to the respective one or more second requests, at the first intermediary server;

transmitting the one or more second responses from the first intermediary server to the second intermediary server, via the messaging bus;

hashing the one or more second requests and the one or more second responses at the first intermediary server to generate one or more second request hashes and one or more second response hashes, respectively;

adding the one or more second request hashes and the one or more second response hashes to the enriched data record in the blockchain, from the first intermediary server; and

receiving the one or more second responses at the second intermediary server and transmitting the one or more second responses to the second document store.

70. (Previously Presented) The computer implemented method as claimed in claim 69, further comprising the steps of:

hashing the one or more second responses at the second intermediary server to regenerate the one or more second response hashes; and

verifying the one or more second response hashes with the blockchain from the second intermediary server, using the token.

71. (Previously Presented) The computer implemented method as claimed in claim 69, wherein each one of the one or more second requests are:

3001229
JPMC Ex. 1002
Page 286

encrypted with a first public key and signed with a second public key at the second intermediary server, before transmission to the first intermediary server; and

decrypted with a first private key at the first intermediary server after reception from the second intermediary server; and

wherein each one of the one or more second responses are:

encrypted with the second public key and signed with the first public key at the first intermediary server, before transmission to the second intermediary server; and

decrypted with a second private key at the second intermediary server after reception from the first intermediary server.

72. (Previously Presented) The computer implemented method as claimed in claim 68, further comprising the steps of adding the first public key from the first intermediary server into the blockchain and adding the second public key from the second intermediary server into the blockchain.

73. (Previously Presented) A system for processing a financial transaction, the system comprising:

a first intermediary server in a centralised financial system, the first intermediary server being operably connected to a network and a first document store;

a token server operably connected to the network;

a messaging bus in the centralised financial system, the messaging bus being operably connected to the network; and

a blockchain operably connected to the network, the blockchain being a distributed ledger;

wherein the first intermediary server is configured to:

transmit one or more documents pertaining to the financial transaction, to the first document store;

generate an enriched data record from the one or more documents and add the enriched data record into the blockchain;

request generation of a token corresponding to the financial transaction to identify the one or more documents, to the token server, via the messaging bus; and

transmit the token to the first document store;

wherein the token server is configured to:

generate the token and add the token into the blockchain in association with the enriched data record; and

transmit the token to the first intermediary server, via the messaging bus.

74. (Previously Presented) A first intermediary server for use in a centralised financial system to facilitate processing of a financial transaction, operably connected to a network and a first document store, and configured to:

transmit one or more documents pertaining to the financial transaction, to the first document store;

generate an enriched data record from the one or more documents and add the enriched data record into a blockchain being a distributed ledger;

request generation of a token corresponding to the financial transaction to identify the one or more documents, to a token server, via a messaging bus in the centralised financial system; and

transmit the token to the first document store.

75. (Previously Presented) The first intermediary server as claimed in claim 74, further configured to send a first financial message comprising the token, to a second intermediary server in the centralised financial system, indicative of making a payment to a second user.

76. (Previously Presented) The first intermediary server as claimed in claim 74, further configured to transmit the token to a first digital device.

77. (Previously Presented) The first intermediary server as claimed in claim 74, further configured to:

transmit one or more first requests, each comprising the token, to a second intermediary server in the centralised financial system, via the messaging bus; and

receive one or more first responses from the second intermediary server and transmit the one or more first responses to the first document store.

78. (Previously Presented) The first intermediary server as claimed in claim 77, wherein the one or more first responses comprise one or more second regulatory compliance documents pertaining to a second user.

REMARKS/ARGUMENTS

Claims 59-78 are present in this application. By this Amendment, claims 59 and 62 have been amended. Reconsideration in view of the above amendments and the following remarks is respectfully requested.

The Office Action initially contends the claim 61 includes subject matter that is not supported by the certified copies of foreign priority filed with the application. Certified copies of AU 2016900239 and AU 2016901924 have been retrieved by the Patent Office and are viewable in PAIR. The Office Action contends that "the subject matter of claim 61 will be examined with an effective filing date of Feb 14, 2018." Applicants request the Examiner to reconsider the priority date of claim 61 based on the priority documents. Additionally, Applicants note that the subject matter of claim 61 finds clear support in the PCT International application. See, for example, paragraphs [009], [026], [042], [0102] and [0134] and claims 3, 20 and 36. At a minimum, the subject matter should thus benefit from the international filing date of August 12, 2016.

Claim 59 was objected to due to an informality. In claim 59, the typographical error has been corrected. Withdrawal of the objection is requested.

Claim 62 was rejected under 35 U.S.C. §112. Claim 62 has been amended to refer to "a second digital device." Withdrawal of the rejection is requested.

Claims 59, 60, 62-66, 69 and 73-78 were rejected under 35 U.S.C. §103 over U.S. Published Patent Application No. 2016/0342994 to Davis in view of U.S. Published Patent Application No. 2012/0203665 to Morgan. Additionally, claim 61 was rejected under 35 U.S.C. §103 over Davis in view of Morgan and U.S. Published Patent Application No. 2018/0314809 to Mintz; claims 67, 68, 70 and 71 were rejected under 35 U.S.C. §103 over Davis in view of Morgan and U.S. Published Patent Application No. 2009/0307495 to Matsuo; and claim 72 was rejected under 35 U.S.C. §103 over Davis in view of Morgan, Matsuo and U.S. Patent No. 10,346,814 to Pennanen. These rejections are respectfully traversed.

Davis is directed to linking blockchain transactions to privately verified identities. As stated in paragraph [0004] of Davis, the problem Davis is trying to solve is "if the wallet is lost, discarded, or stolen, the associated currency often cannot be recovered by the rightful owner and may be used without their knowledge and permission. Furthermore, because of the anonymous nature of the blockchain, the consumer may be unable to prove their identity and ownership of a

wallet, and thereby have little recourse if their wallet and/or associated currency is stolen." In order to solve this problem, Davis stores blockchain transaction related information in traditional payment systems in order to leverage the capabilities of the traditional payment networks, during blockchain transactions happening on a blockchain network, particularly, balance check (paragraph [0041]), fraud detection, risk and sanction assessment (paragraph [0042]), key storage (paragraph [0043]). Therefore, as set out in paragraph [0043], "the payer 102 does not need to retain possession of a computing device for use in blockchain transactions. For example, the issuer 112 may store the private key on behalf of the payer 102 and any transaction identifiers associated with the payer 102 (e.g., in their blockchain currency account) and may be configured to generate the digital signature and include the generated signature and transaction identifier in transaction messages for blockchain transactions involving the payer 102."

In contrast, the problem addressed according to the described embodiments is, as set out in, for example, paragraph [0004], that "[m]any settlement systems are characterised by effective one-way transmission of the plurality of data in any given financial transaction (for example systems based on SWIFT messaging). If it is subsequently discovered that there are deficiencies in the plurality of data transmitted, time consuming checking and querying operations and correspondence often ensues before the financial transaction can be effected." Also, as stated in, for example, paragraph [0416], "banks have already had significant investment in conventional (SWIFT/ACH/RTGS) messaging systems and a complete abandonment of these messaging systems would not be feasible." In order to address this problem, the described embodiments store information (for example, the token and the associated enriched data) in a blockchain. The information is related to financial transactions happening on the traditional payment networks. This is distinguishable from Davis.

In reference to the specific features objected to in the Office Action, it has been alleged that Davis discloses in paragraphs [0081] and [0082] the feature of *generating an enriched data record from the one or more documents, at the first intermediary server* as defined in claim 59. It should be noted that the enriched data record in claim 59 is generated for the financial transaction that is going to happen on the centralised financial system. As described throughout the patent specification, the financial transaction is between the first intermediary server and the second intermediary server in the centralised financial system. However, as set out in paragraph [0036] of Davis, the network identifier (which is considered in the Office Action to be the

enriched data record), may be "used by the processing server 110 to identify the associated blockchain network 106 for posting of the eventual blockchain transaction." Therefore, the enriched data record in claim 59 and the network identifier of Davis refer to different things.

It has been alleged that Davis discloses in paragraph [0040] the feature of *adding the enriched data record into a blockchain being a distributed ledger, from the first intermediary server* in claim 59. It is true according to paragraph [0040] of Davis that the processing server 110 may initiate the blockchain transaction, but that doesn't mean the processing server 110 adds the enriched data record or the network identifier into the blockchain network 106. The network identifier might be part of the blockchain network 106 eventually; however, it is not added by the processing server 110, but rather is a result of the way that the blockchain network 106 operates.

It has been alleged that Davis discloses in paragraphs [0071] and [0077] the feature of *requesting generation of a token corresponding to the financial transaction to identify the one or more documents, to a token server, from the first intermediary server, via a messaging bus in the centralised financial system* in claim 59. It should be noted that as set out in paragraph [0077] of Davis, the issuer 112 (considered in the Office Action to be the token server in claim 59) receives the transaction identifier from the blockchain network 106. This means the transaction identifier is generated at the blockchain network 106 not the issuer 112. In addition, according to paragraph [0071] of Davis, the processing unit 304 of the issuer 112 generates an authorization response, but the authorization response is to indicate whether the blockchain transaction is approved or not. In other words, the processing server 110 of Davis does not request the issuer 112 to generate the transaction identifier, nor the issuer 112 generates the transaction identifier.

It has been alleged that Davis discloses in paragraphs [0075] and [0077] the feature of *generating the token at the token server and adding the token into the blockchain from the token server in association with the enriched data record* in claim 59. As discussed above, the transaction identifier is not generated by the issuer 112. Further, it is not clear in paragraphs [0075] and [0077] if the transaction identifier is added to the blockchain network 106, and it is not mentioned at all in paragraphs [0075] and [0077] that the transaction identifier is associated with any enriched data record in the blockchain network 106.

Based on the above analysis, Applicants submit that Davis does not disclose at least the following features of claim 59:

generating an enriched data record from the one or more documents, at the first intermediary server;

adding the enriched data record into a blockchain being a distributed ledger, from the first intermediary server;

requesting generation of a token corresponding to the financial transaction to identify the one or more documents, to a token server, from the first intermediary server, via a messaging bus in the centralised financial system; and

generating the token at the token server and adding the token into the blockchain from the token server in association with the enriched data record.

These features are similarly lacking in the other cited prior art documents. As such, Applicants submit that independent claim 59 is novel and non-obvious with respect to the cited references individually or in combination. Similar analyses are also applicable to independent claims 73 and 74.

With regard to the dependent claims, Applicants submit that these claims are allowable at least by virtue of their dependency on an allowable independent claim. Moreover, since claim 61 finds express support at least in the PCT application with an international filing date of August 12, 2016, Applicants submit that Mintz is not prior art, and the rejection of claim 61 is misplaced.

Withdrawal of the rejections is requested.

In view of the foregoing amendments and remarks, Applicants respectfully submit that the claims are patentable over the art of record and that the application is in condition for allowance. Should the Examiner believe that anything further is desirable in order to place the application in condition for allowance, the Examiner is invited to contact Applicants' undersigned attorney at the telephone number listed below.

Prompt passage to issuance is earnestly solicited.

The Commissioner is hereby authorized to charge any deficiency, or credit any overpayment, in the fee(s) filed, or asserted to be filed, or which should have been filed herewith (or with any paper hereafter filed in this application by this firm) to Deposit Account No. 14-1140.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: /Alan M. Kagen/
Alan M. Kagen
Reg. No. 36,178

AMK:jls
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100

Electronic Patent Application Fee Transmittal

Application Number:	15752711
Filing Date:	14-Feb-2018
Title of Invention:	COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR
First Named Inventor/Applicant Name:	Nick Armstrong
Filer:	Alan Mark Kagen/Janet Stoy
Attorney Docket Number:	AMK-5243-9

Filed as Small Entity

Filing Fees for U.S. National Stage under 35 USC 371

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 3 months with $0 paid	2253	1	700	700
Miscellaneous:				
			Total in USD ($)	**700**

Electronic Acknowledgement Receipt

EFS ID:	39215282
Application Number:	15752711
International Application Number:	
Confirmation Number:	5327
Title of Invention:	COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR
First Named Inventor/Applicant Name:	Nick Armstrong
Customer Number:	23117
Filer:	Alan Mark Kagen/Janet Stoy
Filer Authorized By:	Alan Mark Kagen
Attorney Docket Number:	AMK-5243-9
Receipt Date:	21-APR-2020
Filing Date:	14-FEB-2018
Time Stamp:	11:15:01
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$700
RAM confirmation Number	E20204KB15168737
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		5243-9_amd.pdf	64294 0e814c06c451cb2280d44bf96cb6587f7fcc1015	yes	12

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	7
	Applicant Arguments/Remarks Made in an Amendment	8	12

Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30872 5ca0d375e11d0a797ba5eee21814efb0b6bc4f2e	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	95166	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/752,711	02/14/2018	Nick Armstrong	AMK-5243-9	5327

23117 7590 10/21/2019

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
MARSH, JORDAN W	

ART UNIT	PAPER NUMBER
3691	

NOTIFICATION DATE	DELIVERY MODE
10/21/2019	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTOMAIL@nixonvan.com
pair_nixon@firsttofile.com

Office Action Summary	Application No. 15/752,711	Applicant(s) Armstrong et al.	
	Examiner JORDAN W MARSH	Art Unit 3691	AIA (FITF) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 14 February 2018.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL.** 2b) ☑ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 59-78 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 59-78 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☑ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☑ Some** c)☐ None of the:

1.☑ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☑ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

/JORDAN W MARSH/
Examiner, Art Unit 3691

Notice of Pre-AIA or AIA Status

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Priority

2. Claim 61 includes subject matter that is not supported by the certified copies of foreign priority filed with the application. Therefore, the subject matter in claim 61 will be examined with an effective filing date of Feb 14, 2018.

3. Acknowledgment is made of applicant's claim for foreign priority based on an application filed in Australia on January 27, 2016. It is noted, however, that applicant has not filed a certified copy of the AU2016900239 application as required by 37 CFR 1.55.

4. Acknowledgment is made of applicant's claim for foreign priority based on an application filed in Australia on May 20, 2016. It is noted, however, that applicant has not filed a certified copy of the AU2016901924 application as required by 37 CFR 1.55.

Claim Objections

5. Claim 59 objected to because of the following informalities: the word "server" is misspelled as "sever" in the 7th line of claim 59. Appropriate correction is required.

Claim Rejections - 35 USC § 112

6. The following is a quotation of 35 U.S.C. 112(b):

> (b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claim 62 rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

8. Claim 62 recites the limitation "the second digital device" in the 5th to last line of the claim. There is insufficient antecedent basis for this limitation in the claim. For examination purposes and to promote compact prosecution, “the second digital device” will be interpreted as a device separate from the first digital device being used by the first user.

Claim Rejections - 35 USC § 103

9. In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

10. The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

> A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

11. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103 are summarized as follows:

1. Determining the scope and contents of the prior art.

2. Ascertaining the differences between the prior art and the claims at issue.

3. Resolving the level of ordinary skill in the pertinent art.

4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

12. Claims 59-60, 62-66, 69, 73-78 is/are rejected under 35 U.S.C. 103 as being unpatentable over Davis; Steven Charles (US 20160342994 A1) hereinafter Davis in view of Morgan; Robert E. et al. (US 20120203665 A1) hereinafter Morgan.

Claim 59

The following limitations are disclosed by Davis:

A computer implemented method for processing a financial transaction, the method comprising the steps of:

generating an enriched data record from the one or more documents, at the first intermediary server, (See [0081] which states that the processing unit 204, as part of the intermediary server, may encode the network identifier. Then in [0082] this encoded, or enriched, data record helps generate a transaction message that is transmitted to the issuer.)

and adding the enriched data record into a blockchain being a distributed ledger, from the first intermediary sever; (See [0040] with reference to fig. 1. This states that the processing server 110, which is intermediary to a payer and payee, may initiate a blockchain transaction.)

requesting generation of a token corresponding to the financial transaction to identify the one or more documents, to a token server, from the first intermediary server, via a messaging bus in the centralised financial system; (See [0071] which states that the receiving

unit 302 may receive a transaction message from the processing server 110 and that an authorization response is generated at the issuer 112. [0077] states that a "transaction identifier" is included in the authorization response message.)

generating the token at the token server and adding the token into the blockchain from the token server in association with the enriched data record; (See [0075] which states that the authorization response, or token, is generated. This authorization response includes a "transaction identifier" as described in [0077].)

transmitting the token to the first intermediary server from the token server, via the messaging bus; (See [0076] which states that the token, in step 408 of fig. 4, is transmitted to the processing server 110.)

and transmitting the token from the first intermediary server to the first document store in association with the one or more documents. (See [0096] which states that linkage data is stored in part 718 after receiving a transaction message from the issuing server in part 702. The linkage data helps associate the blockchain transaction.)

Davis discloses the generation of an enriched data record at a server, adding this record to the blockchain, and requesting generation of a token at a token server. Davis, however, does not disclose the following limitation while Morgan does teach the following limitation:

transmitting one or more documents pertaining to the financial transaction, from a first intermediary server in a centralised financial system to a first document store; (See [0078] which teaches that the

payment processor saves a receipt of the transaction in the purchase history database 112.)

Morgan teaches that a document pertaining to a financial transaction is saved in a first document store. It would have been obvious to one of ordinary skill in the art at the effective filing date of the invention to include the copy of a transaction in a first storage of Morgan into the blockchain-enabled centralized financial system of Davis because the claimed invention amounts to a combination of old elements with a predictable expectation of success, and in the combination the old elements would perform the same function as they do separately. Examiner interprets this scenario to be similar to a person saving a receipt for a typical transaction in their personal records, only in that the transaction is now being recorded on a blockchain. One of ordinary skill in the art at the effective filing date of the invention would have been motivated to make this combination so that a record of the blockchain transaction could be stored in a traditional database.

Claims 60 and 75

The following limitations are further disclosed by Davis:

The computer implemented method as claimed in claim 59, further comprising the step of sending a first financial message comprising the token, from the first intermediary server to a second intermediary server in the centralised financial system, indicative of making a payment to a second user. (See part 412 of fig. 4 which says that the response message, with its transaction identifier described in [0077], is transferred to an acquirer 114. This acquirer 114 is another intermediary server in the system described in fig. 1.)

Claim 62

The following limitations are disclosed by Davis:

Most of the limitations of claim 59, upon which claim 62 depends.

Davis discloses the generation of an enriched data record at a server, adding this record to the blockchain, and requesting generation of a token at a token server. Davis, however, does not disclose the following limitation while Morgan does teach the following limitation:

Some of the limitations of claim 59, upon which claim 62 depends.

The computer implemented method as claimed in claim 59, further comprising the steps of:

transmitting the token from the first intermediary server to a first digital device available with a first user; (See [0055] which states that a QR code, or token, may be generated by a backend server and sent to a POS device for presentation to a customer. Also see part 208 of fig. 2A.)

providing the token to a second user, by the first user; (See [0063] which states that a consumer may scan the QR code generated by the merchant.)

providing the token to a second intermediary server in the centralised financial system, from the second digital device; (See [0071] which states that the consumer sends an authorization request to the consumer's payment processor. [0072] states that the authorization request includes the URL generated from the QR code.)

transmitting the token to a second document store, from the second intermediary server; (See [0078] which teaches that the payment

processor saves a receipt of the transaction in the purchase history database 112.)

and sending a second financial message comprising the token, from the second intermediary server to the first intermediary server, indicative of making a payment to the first user. (See [0075] which teaches that the payment processor sends a response to a server coupled to the POS device.)

Morgan teaches that a token indicative of a financial payment may be sent from a centralized financial system to the device of a first user and shared with a second user. It would have been obvious to one of ordinary skill in the art at the effective filing date of the invention to include the copy of a transaction in a first storage of Morgan into the blockchain-enabled centralized financial system of Davis because the claimed invention amounts to a combination of old elements with a predictable expectation of success, and in the combination the old elements would perform the same function as they do separately. Examiner interprets this scenario to be similar to a consumer-generated QR code used to effect a payment. One of ordinary skill in the art at the effective filing date of the invention would have been motivated to make this combination so that a blockchain transaction could be easily performed between two transacting parties.

Claim 63

The following limitations are further disclosed by Davis:

The computer implemented method as claimed in claim 59, wherein the step of generating the enriched data record comprises:

extracting a plurality of attributes from the one or more documents, at the first intermediary server; (See [0079] which states that a

transaction request includes a plurality of characteristics like a network identifier, a transaction amount, and a public key among others. The processing server 110 receives this information and extracts or uses it.) **and combining the plurality of attributes to generate the enriched data record, at the first intermediary server.** (See [0080]-[0082] which states that the processing unit 204, part of processing server 110, generates an address identifier and encodes a network identifier before a transaction message is generated. The process of going from a transaction request to a transaction message constitutes generated an enriched data record.)

Claim 64

The following limitations are further disclosed by Davis:

The computer implemented method as claimed in claim 59, wherein the step of generating the enriched data record comprises:

extracting a plurality of attributes from the one or more documents, at the first intermediary server; (See [0079] which states that a transaction request includes a plurality of characteristics like a network identifier, a transaction amount, and a public key among others. The processing server 110 receives this information and extracts or uses it.) **de-identifying the plurality of attributes to obtain a plurality of de-identified attributes, at the first intermediary server;** (See [0061] which contemplates encoding the network identifier or any other rule requiring coding can be done by using hashing algorithms. This encoding or encrypting may be considered de-identifying the data.)

and combining the plurality of de-identified attributes to generate the enriched data record, at the first intermediary server. (See [0080]-[0082] which states that the processing unit 204, part of processing server 110, generates an address identifier and encodes a network identifier before a transaction message is generated. The process of going from a transaction request to a transaction message constitutes generated an enriched data record.)

Claim 65

The following limitations are further disclosed by Davis:

The computer implemented method as claimed in claim 59, wherein the step of generating the enriched data record comprises:

extracting a plurality of attributes from the one or more documents, at the first intermediary server; (See [0079] which states that a transaction request includes a plurality of characteristics like a network identifier, a transaction amount, and a public key among others. The processing server 110 receives this information and extracts or uses it.)

hashing the plurality of attributes to generate a plurality of respective hashes, at the first intermediary server; (See [0061] which contemplates encoding the network identifier or any other rule requiring coding can be done by using hashing algorithms.)

and combining the plurality of hashes to generate the enriched data record, at the first intermediary server. (See [0080]-[0082] which states that the processing unit 204, part of processing server 110, generates an address identifier and encodes a network identifier before a transaction

message is generated. The process of going from a transaction request to a transaction message constitutes generated an enriched data record.)

Claim 66

The following limitations are disclosed by Davis:

hashing the one or more first requests and the one or more first responses at the second intermediary server to generate one or more first request hashes and one or more first response hashes, respectively; (See [0052] which teaches the hashing of a destination address in a transaction request and [0061] teaches the hashing of other data all at the same processing server 110.)

adding the one or more first request hashes and the one or more first response hashes to the enriched data record in the blockchain, from the second intermediary server; (See [0040] with reference to fig. 1. This states that the processing server 110, which is intermediary to a payer and payee, may initiate a blockchain transaction. [0061] teaches that the processing server hashes information that is added to the blockchain.)

Davis discloses the generation of an enriched data record at a server, adding this record to the blockchain, and requesting generation of a token at a token server. Davis, however, does not disclose the following limitation while Morgan does teach the following limitations:

transmitting one or more first requests, each comprising the token, from the first intermediary server to a second intermediary server in the centralised financial system, via the messaging bus; (See [0074] which states that the

payment processor receives a request. In [0075] it states that this may come from a server connected to the POS device.)

receiving the one or more first requests at the second intermediary server and transmitting the one or more first requests and the token from the second intermediary server to a second document store; (See [0078] which teaches that the payment processor saves a receipt of the transaction in the purchase history database 112.)

generating one or more first responses, each comprising the token, corresponding to the respective one or more first requests, at the second intermediary server; (See [0074]-[0075] which states that the payment processor processes a request and then generates a response according to the request.)

transmitting the one or more first responses from the second intermediary server to the first intermediary server, via the messaging bus; (See [0074]-[0075] which states that the payment processor transmits a response to the server connected to the POS device.)

and receiving the one or more first responses at the first intermediary server and transmitting the one or more first responses to the first document store. (See [0076] which states that the merchant website server receives the response and transmits an email or a text which acts as a document store for the transaction record.)

Morgan teaches that a token indicative of a financial payment may be sent from a centralized financial system to the device of a first user and shared with a second user. It would have been obvious to one of ordinary skill in the art at the effective filing date of

the invention to include the copy of a transaction in a first storage of Morgan into the blockchain-enabled centralized financial system of Davis because the claimed invention amounts to a combination of old elements with a predictable expectation of success, and in the combination the old elements would perform the same function as they do separately. Examiner interprets this scenario to be similar to a consumer-generated QR code used to effect a payment. One of ordinary skill in the art at the effective filing date of the invention would have been motivated to make this combination so that a blockchain transaction could be easily performed between two transacting parties.

Claim 69

The following limitations are disclosed by Davis:

hashing the one or more second requests and the one or more second responses at the first intermediary server to generate one or more second request hashes and one or more second response hashes, respectively; (See [0052] which teaches the hashing of a destination address in a transaction request and [0061] teaches the hashing of other data all at the same processing server 110.)

adding the one or more second request hashes and the one or more second response hashes to the enriched data record in the blockchain, from the first intermediary server; (See [0040] with reference to fig. 1. This states that the processing server 110, which is intermediary to a payer and payee, may initiate a blockchain transaction. [0061] teaches that the processing server hashes information that is added to the blockchain.)

Davis discloses the generation of an enriched data record at a server, adding this record to the blockchain, and requesting generation of a token at a token server.

Davis, however, does not disclose the following limitation while Morgan does teach the following limitations:

transmitting one or more second requests, each comprising the token, from a second intermediary server in the centralised financial system to the first intermediary server, via the messaging bus; (See [0074] which states that the payment processor receives a request. In [0075] it states that this may come from a server connected to the POS device.)

receiving the one or more second requests at the first intermediary server and transmitting the one or more second requests from the first intermediary server to the first document store; (See [0078] which teaches that the payment processor saves a receipt of the transaction in the purchase history database 112.)

generating one or more second responses, each comprising the token, corresponding to the respective one or more second requests, at the first intermediary server; (See [0074]-[0075] which states that the payment processor processes a request and then generates a response according to the request.)

transmitting the one or more second responses from the first intermediary server to the second intermediary server, via the messaging bus; (See [0074]-[0075] which states that the payment processor transmits a response to the server connected to the POS device.)

and receiving the one or more second responses at the second intermediary server and transmitting the one or more second responses to the second document store. (See [0076] which states that the merchant website server

receives the response and transmits an email or a text which acts as a document store for the transaction record.)

Morgan teaches that a token indicative of a financial payment may be sent from a centralized financial system to the device of a first user and shared with a second user. It would have been obvious to one of ordinary skill in the art at the effective filing date of the invention to include the copy of a transaction in a first storage of Morgan into the blockchain-enabled centralized financial system of Davis because the claimed invention amounts to a combination of old elements with a predictable expectation of success, and in the combination the old elements would perform the same function as they do separately. Examiner interprets this scenario to be similar to a consumer-generated QR code used to effect a payment. One of ordinary skill in the art at the effective filing date of the invention would have been motivated to make this combination so that a blockchain transaction could be easily performed between two transacting parties.

Claim 73

The following limitations are disclosed by Davis:

a first intermediary server in a centralised financial system, the first intermediary server being operably connected to a network and a first document store; (See fig. 1, part 108 and 110. This constitutes a first intermediary server connected to a network. Fig. 2 shows the inside of the first intermediary server that is connected to a first document store in the form of part 212 and 214.)

a token server operably connected to the network; (See fig. 1, part 112 which constitutes the token server.)

a messaging bus in the centralised financial system, the messaging bus being operably connected to the network; (See fig. 2 with its connections between server components, along with fig. 1 and its connections between each of the components in the centralised financial system.)

and a blockchain operably connected to the network, the blockchain being a distributed ledger; (See fig. 1, part 106 which shows a blockchain connected to the network.)

wherein the first intermediary server is configured to:

generate an enriched data record from the one or more documents and add the enriched data record into the blockchain; (See [0081] which states that the processing unit 204, as part of the intermediary server, may encode the network identifier. Then in [0082] this encoded, or enriched, data record helps generate a transaction message that is transmitted to the issuer.)

request generation of a token corresponding to the financial transaction to identify the one or more documents, to the token server, via the messaging bus; (See [0071] which states that the receiving unit 302 may receive a transaction message from the processing server 110 and that an authorization response is generated at the issuer 112. [0077] states that a "transaction identifier" is included in the authorization response message.)

and transmit the token to the first document store; (See [0096] which states that linkage data is stored in part 718 after receiving a transaction

message from the issuing server in part 702. The linkage data helps associate the blockchain transaction.)

Davis discloses the generation of an enriched data record at a server, adding this record to the blockchain, and requesting generation of a token at a token server. Davis, however, does not disclose the following limitation while Morgan does teach the following limitations:

transmit one or more documents pertaining to the financial transaction, to the first document store; (See [0078] which teaches that the payment processor saves a receipt of the transaction in the purchase history database 112.)

Morgan teaches that a document pertaining to a financial transaction is saved in a first document store. It would have been obvious to one of ordinary skill in the art at the effective filing date of the invention to include the copy of a transaction in a first storage of Morgan into the blockchain-enabled centralized financial system of Davis because the claimed invention amounts to a combination of old elements with a predictable expectation of success, and in the combination the old elements would perform the same function as they do separately. Examiner interprets this scenario to be similar to a person saving a receipt for a typical transaction in their personal records, only in that the transaction is now being recorded on a blockchain. One of ordinary skill in the art at the effective filing date of the invention would have been motivated to make this combination so that a record of the blockchain transaction could be stored in a traditional database.

Claim 74

The following limitations are disclosed by Davis:

A first intermediary server for use in a centralised financial system to facilitate processing of a financial transaction, operably connected to a network and a first document store, and configured to:

generate an enriched data record from the one or more documents and add the enriched data record into a blockchain being a distributed ledger; (See [0081] which states that the processing unit 204, as part of the intermediary server, may encode the network identifier. Then in [0082] this encoded, or enriched, data record helps generate a transaction message that is transmitted to the issuer.)

request generation of a token corresponding to the financial transaction to identify the one or more documents, to a token server, via a messaging bus in the centralised financial system; (See [0071] which states that the receiving unit 302 may receive a transaction message from the processing server 110 and that an authorization response is generated at the issuer 112. [0077] states that a "transaction identifier" is included in the authorization response message.)

and transmit the token to the first document store. (See [0096] which states that linkage data is stored in part 718 after receiving a transaction message from the issuing server in part 702. The linkage data helps associate the blockchain transaction.)

Davis discloses the generation of an enriched data record at a server, adding this record to the blockchain, and requesting generation of a token at a token server.

Davis, however, does not disclose the following limitation while Morgan does teach the following limitations:

transmit one or more documents pertaining to the financial transaction, to the first document store; (See [0078] which teaches that the payment processor saves a receipt of the transaction in the purchase history database 112.)

Morgan teaches that a document pertaining to a financial transaction is saved in a first document store. It would have been obvious to one of ordinary skill in the art at the effective filing date of the invention to include the copy of a transaction in a first storage of Morgan into the blockchain-enabled centralized financial system of Davis because the claimed invention amounts to a combination of old elements with a predictable expectation of success, and in the combination the old elements would perform the same function as they do separately. Examiner interprets this scenario to be similar to a person saving a receipt for a typical transaction in their personal records, only in that the transaction is now being recorded on a blockchain. One of ordinary skill in the art at the effective filing date of the invention would have been motivated to make this combination so that a record of the blockchain transaction could be stored in a traditional database.

Claim 76

The following limitations are disclosed by Davis:

Most of the limitations of claim 74, upon which claim 76 depends.

Davis discloses the generation of an enriched data record at a server, adding this record to the blockchain, and requesting generation of a token at a token server.

Davis, however, does not disclose the following limitation while Morgan does teach the following limitations:

Some of the limitations of claim 74, upon which claim 76 depends.

The first intermediary server as claimed in claim 74, further configured to transmit the token to a first digital device. (See [0055] which states that a QR code may be generated by a backend server and then sent to a POS device for presentation to the consumer.)

Morgan teaches that a document pertaining to a financial transaction is saved in a first document store. It would have been obvious to one of ordinary skill in the art at the effective filing date of the invention to include the copy of a transaction in a first storage of Morgan into the blockchain-enabled centralized financial system of Davis because the claimed invention amounts to a combination of old elements with a predictable expectation of success, and in the combination the old elements would perform the same function as they do separately. Examiner interprets this scenario to be similar to a person saving a receipt for a typical transaction in their personal records, only in that the transaction is now being recorded on a blockchain. One of ordinary skill in the art at the effective filing date of the invention would have been motivated to make this combination so that a record of the blockchain transaction could be stored in a traditional database.

Claim 77

The following limitations are disclosed by Davis:

Most of the limitations of claim 74, upon which claim 77 depends.

Davis discloses the generation of an enriched data record at a server, adding this record to the blockchain, and requesting generation of a token at a token server. Davis, however, does not disclose the following limitation while Morgan does teach the following limitations:

Some of the limitations of claim 74, upon which claim 77 depends.

The first intermediary server as claimed in claim 74, further configured to:

transmit one or more first requests, each comprising the token, to a second intermediary server in the centralised financial system, via the messaging bus; (See [0074] which states that the payment processor receives a request. In [0075] it states that this may come from a server connected to the POS device.)

and receive one or more first responses from the second intermediary server and transmit the one or more first responses to the first document store. (See [0076] which states that the merchant website server receives the response and transmits an email or a text which acts as a document store for the transaction record.)

Morgan teaches that a document pertaining to a financial transaction is saved in a first document store. It would have been obvious to one of ordinary skill in the art at the effective filing date of the invention to include the copy of a transaction in a first storage of Morgan into the blockchain-enabled centralized financial system of Davis because the claimed invention amounts to a combination of old elements with a predictable expectation of success, and in the combination the old elements would perform the same function as they do separately. Examiner interprets this scenario to be similar to a person saving a receipt for a typical transaction in their personal records, only in that the transaction is now being recorded on a blockchain. One of ordinary skill in the art at the effective filing date of the invention would have been motivated to make this combination so that a record of the blockchain transaction could be stored in a traditional database.

Claim 78

The following limitations are further disclosed by Davis:

The first intermediary server as claimed in claim 77, wherein the one or more first responses comprise one or more second regulatory compliance documents pertaining to a second user. (See [0076] which states that an authorization response may be formatted, "based on the one or more standards". A standard may be reasonably interpreted as a regulatory function.)

13. Claim 61 is/are rejected under 35 U.S.C. 103 as being unpatentable over Davis in view of Morgan and further in view of Mintz; Kevin Matthew et al. (US 20180314809 A1) hereinafter Mintz.

Claim 61

The following limitations are disclosed by Davis:

Most of the limitations of claim 59, upon which claim 61 depends.

Davis discloses the generation of an enriched data record at a server, adding this record to the blockchain, and requesting generation of a token at a token server. Davis, however, does not disclose the following limitation while Morgan does teach the following limitations:

Some of the limitations of claim 59, upon which claim 61 depends.

Please see the response to claim 59 to see the Graham v. Deere motivation statement for combining the Davis and Morgan references.

Morgan teaches that a document pertaining to a financial transaction is saved in a first document store. Davis and Morgan together, however, do not disclose the following limitation while Mintz does teach the following limitations:

The computer implemented method as claimed in claim 59, further comprising the steps of:

implementing a smart contract at the token server; (See [0020] which states that a server node may generate a smart contract.)

and adding the smart contract into the blockchain, from the token server. (See [0020] which states that this server node may append the smart contract to a blockchain.)

Mintz teaches that a smart contract can be implemented at a server and added to the blockchain. It would have been obvious to one of ordinary skill in the art at the effective filing date of the invention to include in the centralized blockchain financial system of Davis and Morgan the implementation of a smart contract into the blockchain by a server as in Mintz because the claimed invention amounts to a combination of old elements, and in the combination the old elements would perform the same function as they do separately. One of ordinary skill in the art at the effective filing date of the invention would have been motivated to make this combination so that the advantages of smart contracts could be included within a user accessible blockchain transaction system.

14. Claims 67-68 and 70-71 is/are rejected under 35 U.S.C. 103 as being unpatentable over Davis in view of Morgan and further in view of Matsuo; Masakatsu (20090307495 A1) hereinafter Matsuo.

Claim 67

The following limitations are disclosed by Davis:

Most of the limitations of claim 59, upon which claim 67 depends.

Some of the limitations of claim 66, upon which claim 67 depends.

The computer implemented method as claimed in claim 66, further comprising the steps of:

and verifying the one or more first response hashes with the blockchain from the first intermediary server, using the token. (See fig. 4, part 416 which teaches the verification of a blockchain transaction with its accompanying hashes. Also see [0077] for the description of this verification step.)

Davis discloses the generation of an enriched data record at a server, adding this record to the blockchain, and requesting generation of a token at a token server. Davis, however, does not disclose the following limitation while Morgan does teach the following limitations:

Some of the limitations of claim 59, upon which claim 67 depends.

Most of the limitations of claim 66, upon which claim 67 depends.

Morgan teaches that a document pertaining to a financial transaction is saved in a first document store. Davis and Morgan together, however, do not disclose the following limitation while Matsuo does teach the following limitations:

hashing the one or more first responses at the first intermediary server to regenerate the one or more first response hashes; (See fig. 12, part 11 which teaches the hashing a response from a client at a server.)

Matsuo teaches that a response may be hashed at a server from a client. It would have been obvious to one of ordinary skill in the art at the effective filing date of the invention to include in the blockchain-enabled financial system of Davis and Morgan the ability to hash a response at a server as in Matsuo because the claimed invention is merely a combination of old elements with a predictable expectation of success, and in the combination the old elements would perform the same function as they do separately. One of ordinary skill in the art at the effective filing date of the invention

would have been motivated to make this combination to ensure that request and response messages from in-network servers would be protected by hashing from outside hackers.

Claim 68

The following limitations are disclosed by Davis:

Most of the limitations of claim 59, upon which claim 68 depends.

Some of the limitations of claim 66, upon which claim 68 depends.

Davis discloses the generation of an enriched data record at a server, adding this record to the blockchain, and requesting generation of a token at a token server. Davis, however, does not disclose the following limitation while Morgan does teach the following limitations:

Some of the limitations of claim 59, upon which claim 68 depends.

Most of the limitations of claim 66, upon which claim 68 depends.

Please see the responses to claim 59 and 66 to see the Graham v. Deere motivation statements for combining the Davis and Morgan references.

Morgan teaches that a document pertaining to a financial transaction is saved in a first document store. Davis and Morgan together, however, do not disclose the following limitation while Matsuo does teach the following limitations:

The computer implemented method as claimed in claim 66, wherein each one of the one or more first requests are:

encrypted with a second public key and signed with a first public key at the first intermediary server, before transmission to the second intermediary server; (See fig. 8, part 2 which teaches encryption with a

public key. Then see part 3 which teaches encryption with a password, which could reasonably be interpreted as a signature.)

and decrypted with a second private key at the second intermediary server after reception from the first intermediary server; (See part 7 of fig. 8, which teaches decryption with a private key after reception of a message from the client.)

and wherein each one of the one or more first responses are:

encrypted with the first public key and signed with the second public key at the second intermediary server, before transmission to the first intermediary server; (See fig. 8, part 2 which teaches encryption with a public key. Then see part 3 which teaches encryption with a password, which could reasonably be interpreted as a signature.)

and decrypted with a first private key at the first intermediary server after reception from the second intermediary server. (See part 7 of fig. 8, which teaches decryption with a private key after reception of a message from the client.)

Matsuo teaches that a response may be hashed at a server from a client. It would have been obvious to one of ordinary skill in the art at the effective filing date of the invention to include in the blockchain-enabled financial system of Davis and Morgan the ability to encrypt and decrypt keys at a server as in Matsuo because the claimed invention is merely a combination of old elements with a predictable expectation of success, and in the combination the old elements would perform the same function as they do separately. One of ordinary skill in the art at the effective filing date of the

invention would have been motivated to make this combination to ensure that request and response messages from in-network servers would be protected by hashing from outside hackers.

Claim 70

The following limitations are disclosed by Davis:

Most of the limitations of claim 59, upon which claim 70 depends.

Some of the limitations of claim 69, upon which claim 70 depends.

The computer implemented method as claimed in claim 69, further comprising the steps of:

and verifying the one or more second response hashes with the blockchain from the first intermediary server, using the token. (See fig. 4, part 416 which teaches the verification of a blockchain transaction with its accompanying hashes. Also see [0077] for the description of this verification step.)

Davis discloses the generation of an enriched data record at a server, adding this record to the blockchain, and requesting generation of a token at a token server. Davis, however, does not disclose the following limitation while Morgan does teach the following limitations:

Some of the limitations of claim 59, upon which claim 70 depends.

Most of the limitations of claim 69, upon which claim 70 depends.

Morgan teaches that a document pertaining to a financial transaction is saved in a first document store. Davis and Morgan together, however, do not disclose the following limitation while Matsuo does teach the following limitations:

hashing the one or more second responses at the second intermediary server to regenerate the one or more second response hashes; (See fig. 12, part 11 which teaches the hashing a response from a client at a server.)

Matsuo teaches that a response may be hashed at a server from a client. It would have been obvious to one of ordinary skill in the art at the effective filing date of the invention to include in the blockchain-enabled financial system of Davis and Morgan the ability to hash a response at a server as in Matsuo because the claimed invention is merely a combination of old elements with a predictable expectation of success, and in the combination the old elements would perform the same function as they do separately. One of ordinary skill in the art at the effective filing date of the invention would have been motivated to make this combination to ensure that request and response messages from in-network servers would be protected by hashing from outside hackers.

Claim 71

The following limitations are disclosed by Davis:

Most of the limitations of claim 59, upon which claim 71 depends.

Some of the limitations of claim 69, upon which claim 71 depends.

Davis discloses the generation of an enriched data record at a server, adding this record to the blockchain, and requesting generation of a token at a token server. Davis, however, does not disclose the following limitation while Morgan does teach the following limitations:

Some of the limitations of claim 59, upon which claim 71 depends.

Most of the limitations of claim 69, upon which claim 71 depends.

Morgan teaches that a document pertaining to a financial transaction is saved in a first document store. Davis and Morgan together, however, do not disclose the following limitation while Matsuo does teach the following limitations:

The computer implemented method as claimed in claim 69, wherein each one of the one or more second requests are:

encrypted with a first public key and signed with a second public key at the second intermediary server, before transmission to the first intermediary server; (See fig. 8, part 2 which teaches encryption with a public key. Then see part 3 which teaches encryption with a password, which could reasonably be interpreted as a signature.)

and decrypted with a first private key at the first intermediary server after reception from the second intermediary server; (See part 7 of fig. 8, which teaches decryption with a private key after reception of a message from the client.)

and wherein each one of the one or more second responses are:

encrypted with the second public key and signed with the first public key at the first intermediary server, before transmission to the second intermediary server; (See fig. 8, part 2 which teaches encryption with a public key. Then see part 3 which teaches encryption with a password, which could reasonably be interpreted as a signature.)

and decrypted with a second private key at the second intermediary server after reception from the first intermediary

server. (See part 7 of fig. 8, which teaches decryption with a private key after reception of a message from the client.)

Matsuo teaches that a request with its appropriate keys may be encrypted and decrypted for security. It would have been obvious to one of ordinary skill in the art at the effective filing date of the invention to include in the blockchain-enabled financial system of Davis and Morgan the ability to hash a response at a server as in Matsuo because the claimed invention is merely a combination of old elements with a predictable expectation of success, and in the combination the old elements would perform the same function as they do separately. One of ordinary skill in the art at the effective filing date of the invention would have been motivated to make this combination to ensure that request and response messages from in-network servers would be protected by hashing from outside hackers.

15. Claim 72 is/are rejected under 35 U.S.C. 103 as being unpatentable over Davis in view of Morgan in view of Matsuo and further in view of Pennanen; Antti (US 10346814 B2) hereinafter Pennanen.

Claim 72

The following limitations are disclosed by Davis:

Most of the limitations of claim 59, upon which claim 72 depends.

Some of the limitations of claim 66, upon which claim 72 depends.

Davis discloses the generation of an enriched data record at a server, adding this record to the blockchain, and requesting generation of a token at a token server.

Davis, however, does not disclose the following limitation while Morgan does teach the following limitations:

Some of the limitations of claim 59, upon which claim 72 depends.

Most of the limitations of claim 66, upon which claim 72 depends.

Please see the response to claim 59 to view the Graham v. Deere motivation statement for combining the Davis and Morgan references.

Morgan teaches that a document pertaining to a financial transaction is saved in a first document store. Davis and Morgan together, however, do not disclose the following limitations while Matsuo does teach the following limitations:

All of the limitations of claim 68, upon which claim 72 depends.

Please see the response to claim 68 to view to Graham v. Deere motivation statements for combining the Davis, Morgan, and Matsuo references.

Matsuo teaches that a request with its appropriate keys may be encrypted and decrypted for security. Davis, Morgan, and Matsuo together, however, do not disclose the following limitations while Pennanen does teach the following limitations:

The computer implemented method as claimed in claim 68, further comprising the steps of adding the first public key from the first intermediary server into the blockchain and adding the second public key from the second intermediary server into the blockchain. (See column 4, lines 58-62 which states that a blockchain uses respective payer and payee public keys to identify them on the blockchain record. Then see column 2, lines 2-6 which teach that respective computer servers add their record of their transactions to the copy of the ledger. Thus, different servers add their respective public keys to the blockchain.)

Pennanen teaches that a first public key and second public key for two transacting parties are added to the blockchain from different servers. It would have been obvious to one of ordinary skill in the art at the effective filing date of the invention to modify the teachings of Davis, Morgan, and Matsuo to include the process by which public keys

are entered on the blockchain as in Pennanen because a blockchain transaction record has to have some way to identify the parties involved in a transaction; this limitation describes how that process is performed. One of ordinary skill in the art at the effective filing date of the invention would have been motivated to combine these teachings so that the blockchain transaction record would be capable of being identified and thereby avoid losing track of the parties that agreed to transact.

Conclusion

16. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JORDAN W MARSH whose telephone number is (571)270-7623. The examiner can normally be reached on Mon - Thurs: 6:30am - 4:30pm EST.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Alexander Kalinowski can be reached on (571) 272-6771. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/JORDAN W MARSH/
Examiner, Art Unit 3691

/ABHISHEK VYAS/
Primary Examiner, Art Unit 3691

Notice of References Cited	Application/Control No. 15/752,711	Applicant(s)/Patent Under Reexamination Armstrong et al.	
	Examiner JORDAN W MARSH	Art Unit 3691	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20160342994-A1	11-2016	Davis; Steven Charles	G06Q20/027	1/1
*	B	US-20120203665-A1	08-2012	Morgan; Robert E.	H04W12/06	705/26.41
*	C	US-20180314809-A1	11-2018	Mintz; Kevin Matthew	H04L63/10	1/1
*	D	US-20090307495-A1	12-2009	MATSUO; Masakatsu	H04L9/002	713/171
*	E	US-10346814-B2	07-2019	Pennanen; Antti	G06Q20/4012	1/1
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/752,711	Armstrong et al.
	Examiner	Art Unit
	JORDAN W MARSH	3691

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	10/15/2019								
	59	✓								
	60	✓								
	61	✓								
	62	✓								
	63	✓								
	64	✓								
	65	✓								
	66	✓								
	67	✓								
	68	✓								
	69	✓								
	70	✓								
	71	✓								
	72	✓								
	73	✓								
	74	✓								
	75	✓								
	76	✓								
	77	✓								
	78	✓								

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/752,711	Armstrong et al.
	Examiner	Art Unit
	JORDAN W MARSH	3691

CPC - Searched*		
Symbol	Date	Examiner
G06F 21/64	10/15/2019	JM
G06Q 20/382	10/15/2019	JM
G06Q 20/385	10/15/2019	JM

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
Inventor search	10/15/2019	JM
EAST search history attached	10/15/2019	JM
Consulted with primary examiner Abhishek Vyas	10/15/2019	JM
Used ip.com. Screenshot attached	10/15/2019	JM

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

INFORMATION DISCLOSURE CITATION	ATTY. DOCKET NO.	APPLICATION NO.
	AMK-5243-0009	To Be Assigned
	INVENTOR(S)	
	ARMSTRONG et al.	
(Use several sheets if necessary)	FILING DATE	ART UNIT
	Concurrently Herewith	To be Assigned

U.S. PATENT DOCUMENTS

*EXAMINER INITIALS		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
		2004/0006692	1/2004	Honda et al.			
		2008/0201580	8/2008	Savitzky et al.			
		2009/0100041	4/2009	Wilson			
		2011/0184910	7/2011	Love et al.			
		2014/0279519	9/2014	Mattes et al.			

FOREIGN PATENT DOCUMENTS

*EXAMINER INITIALS		DOCUMENT	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION YES	TRANSLATION NO
		2 843 587	3/2015	Europe				
		WO 2015/116998	8/2015	PCT				

OTHER DOCUMENTS (including Author, Title, Date, Pertinent pages, etc.)

		International Search Report dated November 1, 2016 issued in PCT International Patent Application No. PCT/AU2016/000279, 3 pp.
		Nakamoto, Satoshi et al., "Bitcoin: A Peer-to-Peer Electronic Cash System." (2008). [Retrieved from Internet on 25 October 2016]. URL: http://web.archive.org/web/20150616021417/http://www.cryptovest.co.uk/resources/Bitcoin%20paper%200riginal.pdf, published on or before 16 June 2015 as per Wayback Machine, 9 pp.
		Snow, Paul et al., "Factom Ledger by Consensus," [Retrieved from Internet on 25 October 2016]. URL: http ://bravenewcoin.com/assets/Whitepapers/FactomLedgerbyConsensus.pdf, January 17, 2015, 28 pp.

Examiner Signature	/JORDAN W MARSH/	Date Considered	10/15/2019

*Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.W.M./

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	0	((("Identitii") near3 ("Pty") near3 ("Ltd"))).AS,AANM.	USPAT	OR	ON	2019/09/18 15:32
S2	1	((("Armstrong") near3 ("Nick"))).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2019/09/18 15:33
S3	1	((("Buckingham") near3 ("Ben"))).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2019/09/18 15:33
S4	282	((("Friedman") near3 ("Daniel"))).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2019/09/18 15:33
S5	5	((("Shepherd") near3 ("Elliot"))).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2019/09/18 15:33
S6	36	((("Knight") near3 ("Eric"))).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2019/09/18 15:33
S7	1	"2015013908"	US-PGPUB; USPAT; USOCR	OR	ON	2019/09/18 16:24
S8	2	"20150013908"	US-PGPUB; USPAT; USOCR	OR	ON	2019/09/18 16:25
S9	44	(Kremen near3 Gary)	US-PGPUB; USPAT; USOCR	OR	ON	2019/09/18 16:25
S10	0	WO2015116998	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/09/18 16:57
S11	0	WO20150116998	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/09/18 16:58
S12	0	PCTUS2015013908	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/09/18 16:58
S13	0	PCT2015013908	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	ON	2019/09/18 16:58

			DERWENT; IBM_TDB			
S14	14	"2015013908"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/09/18 16:59
S15	15828344	WO "2017104871"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/09/18 16:59
S16	0	WO2017104871	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/09/18 17:00
S17	0	WO2017104871A2	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/09/18 17:00
S18	14	"2015013908"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/09/18 17:00
S19	14	"2015116998"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/09/18 17:01
S20	1	blockchain and ((first and second) adj intermediary adj server) and (token adj server)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/09/20 07:39
S21	1	S20 AND ((G06F21/64 OR G06Q20/382 OR G06Q20/3823 OR G06Q20/3827 OR G06Q20/385 OR G06Q20/389 OR H04L63/0442 OR H04L63/0471).CPC.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/09/20 07:40
S22	57683	((G06F21/64 OR G06Q20/382 OR G06Q20/3823 OR G06Q20/3827 OR G06Q20/385 OR G06Q20/389 OR H04L63/0442 OR H04L63/0471).CPC.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/09/20 07:40

S23	0	blockchain and ((first and second) adj server) and (token adj server)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/09/20 07:42
S24	2	blockchain and ((first) adj server) and (token adj server)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/09/20 07:42
S25	1	"20140201084"	US-PGPUB; USPAT; USOCR	OR	ON	2019/09/20 07:52
S26	1	"20180293573"	US-PGPUB; USPAT; USOCR	OR	ON	2019/09/20 09:36
S27	1	"20190066228"	US-PGPUB; USPAT; USOCR	OR	ON	2019/09/20 09:40
S28	2	"20170161733"	US-PGPUB; USPAT; USOCR	OR	ON	2019/09/20 09:43
S29	1	"20140214759"	US-PGPUB; USPAT; USOCR	OR	ON	2019/09/20 09:47
S30	1	"20180240112"	US-PGPUB; USPAT; USOCR	OR	ON	2019/09/20 11:59
S31	2	"20040006692"	US-PGPUB; USPAT; USOCR	OR	ON	2019/09/20 12:11
S32	7	"20080201580" "20090100041" "20110184910" "20140279519"	US-PGPUB; USPAT; USOCR	OR	ON	2019/09/20 12:12
S33	0	S31 and S32	US-PGPUB; USPAT; USOCR	OR	ON	2019/09/20 12:12
S34	7	"20080201580" "20090100041" "20110184910" "20140279519" "200400066923"	US-PGPUB; USPAT; USOCR	OR	ON	2019/09/20 12:12
S35	2	(blockchain or (distributed adj ledger)) and ((first) adj server) and (token adj (server or vault or processor or computer or module))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/09/20 12:15
S36	91	(blockchain or (distributed adj ledger)) and (token adj (server or vault or processor or computer or module))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/09/20 12:15
S37	89	S36 and transaction	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	ON	2019/09/20 12:16

			DERWENT; IBM_TDB			
S38	26	S36 and (financial adj transaction)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/09/20 12:17
S39	0	"20190122300"	USPAT	OR	ON	2019/10/03 16:36
S40	1	("20190122300").PN.	US-PGPUB; USPAT	OR	OFF	2019/10/03 16:36
S41	1	("10198769").PN.	US-PGPUB; USPAT	OR	OFF	2019/10/03 16:45
S42	1	("9033798").PN.	US-PGPUB; USPAT	OR	OFF	2019/10/03 16:46
S43	1	("8727869").PN.	US-PGPUB; USPAT	OR	OFF	2019/10/03 16:46
S44	106	"20170046693" "5895450" "20180005186" "20180082390"	US-PGPUB; USPAT	OR	ON	2019/10/03 16:50
S45	0	("20170046693""5895450""20180005186""20180082390").PN.	US-PGPUB; USPAT	OR	OFF	2019/10/03 16:50
S46	0	("20170046693""5895450""20180005186""20180082390").PN.	US-PGPUB; USPAT	OR	OFF	2019/10/03 16:50
S47	1	("20170046693").PN.	US-PGPUB; USPAT	OR	OFF	2019/10/03 16:50
S48	2	"20160342994"	US-PGPUB; USPAT	OR	ON	2019/10/03 17:23
S49	0	(consumer adj (generated or presented)) near3 (QR adj code)	USPAT	OR	ON	2019/10/08 14:06
S50	1	(consumer adj (generated or presented)) with (QR adj code)	USPAT	OR	ON	2019/10/08 14:06
S51	0	(consumer$1generated) with (QR adj code)	USPAT	OR	ON	2019/10/08 14:07
S52	0	(consumer$1presented) with (QR adj code)	USPAT	OR	ON	2019/10/08 14:07
S53	0	((customer or consumer) adj (generated or presented)) near3 (QR or (quick adj response adj code))	USPAT	OR	ON	2019/10/08 14:09
S54	2	((customer or consumer) adj (generated or presented)) with (QR or (quick adj response adj code))	USPAT	OR	ON	2019/10/08 14:10
S55	1	"9953311"	USPAT	OR	ON	2019/10/08 14:44
S56	1	"20110251892"	USPAT	OR	ON	2019/10/08 15:37
S57	0	"20120203665"	USPAT	OR	ON	2019/10/09 09:39
S58	1	("20120203665").PN.	US-PGPUB; USPAT	OR	OFF	2019/10/09 09:39
S59	3	"20160342994"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/10/09 10:06
S60	3	"20090307495"	US-PGPUB; USPAT; USOCR;	OR	ON	2019/10/09 11:31

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S61	14	(smart adj contract) with token with server with blockchain	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/10/09 15:33
S62	70	(smart adj contract) same token same server same blockchain	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/10/09 15:38
S63	60	(smart adj contract) near3 (implement or generate or create or establish or start)	USPAT	OR	ON	2019/10/11 17:25
S64	56	S63 and blockchain	USPAT	OR	ON	2019/10/11 17:25
S65	0	((smart adj contract) near3 (implement or generate or create or establish or start)) with add with blockchain	USPAT	OR	ON	2019/10/11 17:26
S66	7	((smart adj contract) near3 (implement or generate or create or establish or start)) same add same blockchain	USPAT	OR	ON	2019/10/11 17:26
S67	38	S63 and blockchain and token	USPAT	OR	ON	2019/10/11 17:30
S68	7	"9875510"	US-PGPUB; USPAT	OR	ON	2019/10/14 14:35
S69	2	"10346814"	US-PGPUB; USPAT	OR	ON	2019/10/14 15:07
S70	58	(add) with (smart adj contract) with (blockchain)	US-PGPUB; USPAT	OR	ON	2019/10/14 15:37
S71	39	((add) with (smart adj contract) with (blockchain)) and token and server	US-PGPUB; USPAT	OR	ON	2019/10/14 15:37

10/ 15/ 2019 9:58:55 AM
C:\ Users\ jmarsh\ Documents\ EAST\ Workspaces\ 15752711 processing financial transaction.wsp

Bibliographic Data

Application No: 15/752,711

Foreign Priority claimed: (•) Yes ( ) No

35 USC 119 (a-d) conditions met: ( ) Yes (☑) No ( ) Met After Allowance

Verified and Acknowledged: /JORDAN W MARSH/ Examiner's Signature | Initials

Title: COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
02/14/2018	705	3691	AMK-5243-9
RULE			

APPLICANTS

Identitii Pty Ltd, Surry Hills, New South Wales, AUSTRALIA

INVENTORS

Nick Armstrong Sydney, AUSTRALIA

Ben Buckingham Sydney, AUSTRALIA

Daniel Friedman Sydney, AUSTRALIA

Elliot Shepherd Sydney, AUSTRALIA

Eric Knight Sydney, AUSTRALIA

CONTINUING DATA

This application is a 371 of PCT/AU2016/000279 08/12/2016

FOREIGN APPLICATIONS

AUSTRALIA 2015903292 08/14/2015

AUSTRALIA 2016900239 01/27/2016

AUSTRALIA 2016901924 05/20/2016

IF REQUIRED, FOREIGN LICENSE GRANTED**

05/21/2018

**** SMALL ENTITY ****

STATE OR COUNTRY

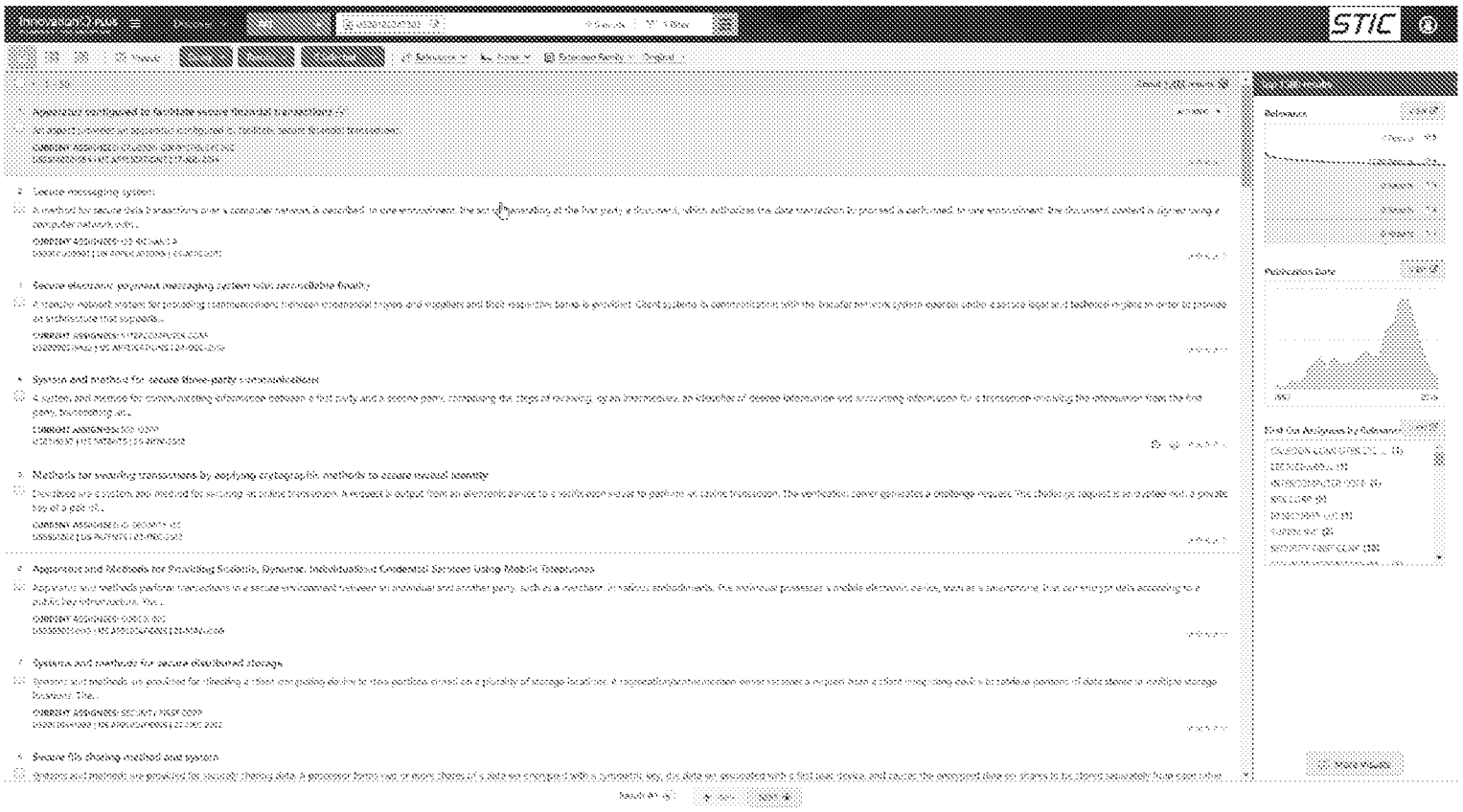
AUSTRALIA

ADDRESS

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203
UNITED STATES

FILING FEE RECEIVED

$1,060



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
15/752,711	02/14/2018	Nick Armstrong	AMK-5243-9

CONFIRMATION NO. 5327

23117
NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

PUBLICATION NOTICE

OC000000101983767

Title:COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR

Publication No.US-2018-0247302-A1
Publication Date:08/30/2018

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Public Records Division. The Public Records Division can be reached by telephone at (571) 272-3150 or (800) 972-6382, by facsimile at (571) 273-3250, by mail addressed to the United States Patent and Trademark Office, Public Records Division, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently https://portal.uspto.gov/pair/PublicPair. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

MULTIPLE DEPENDENT CLAIM FEE CALCULATION SHEET

Substitute for Form PTO-1360
(For use with Form PTO/SB/06)

Application Number	Filing Date
15752711	

Applicant(s) Nick Armstrong

* May be used for additional claims or amendments

CLAIMS	AS FILED		AFTER FIRST AMENDMENT		AFTER SECOND AMENDMENT	
	Indep	Depend	Indep	Depend	Indep	Depend
1	1		---	---		
2		1	---	---		
3		1	---	---		
4		1	---	---		
5		1	---	---		
6		1	---	---		
7		1	---	---		
8		1	---	---		
9		1	---	---		
10		1	---	---		
11		1	---	---		
12		1	---	---		
13		1	---	---		
14		1	---	---		
15		1	---	---		
16		2	---	---		
17		1	---	---		
18	1		---	---		
19		1	---	---		
20		1	---	---		
21		1	---	---		
22		1	---	---		
23		1	---	---		
24		1	---	---		
25		1	---	---		
26		1	---	---		
27		1	---	---		
28		1	---	---		
29		1	---	---		
30		1	---	---		
31		1	---	---		
32		1	---	---		
33		2	---	---		
34		(1)	---	---		
35	1		---	---		
36		1	---	---		
37	1		---	---		
38		1	---	---		
39		1	---	---		
40		1	---	---		
41		1	---	---		
42		1	---	---		
43		1	---	---		
44		1	---	---		
45		1	---	---		
46		1	---	---		
47		1	---	---		
48		1	---	---		
49		1	---	---		
50		2	---	---		
Total Indep	7		3		0	
Total Depend	55	↵	17	↵	0	↵
Total Claims	62		20		0	

	*		*		*	
	Indep	Depend	Indep	Depend	Indep	Depend
51	1		---	---		
52	1		---	---		
53		1	---	---		
54	1		---	---		
55		1	---	---		
56		1	---	---		
57		2	---	---		
58		1	---	---		
59			1			
60				1		
61				1		
62				1		
63				1		
64				1		
65				1		
66				1		
67				1		
68				1		
69				1		
70				1		
71				1		
72				1		
73			1			
74			1			
75				1		
76				1		
77				1		
78				1		
79						
80						
81						
82						
83						
84						
85						
86						
87						
88						
89						
90						
91						
92						
93						
94						
95						
96						
97						
98						
99						
100						

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

U.S. APPLICATION NUMBER NO.	FIRST NAMED INVENTOR	ATTY. DOCKET NO.
15/752,711	Nick Armstrong	AMK-5243-9

23117
NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

INTERNATIONAL APPLICATION NO.	
PCT/AU2016/000279	
I.A. FILING DATE	PRIORITY DATE
08/12/2016	08/14/2015

CONFIRMATION NO. 5327
371 ACCEPTANCE LETTER

OC000000099695030

Date Mailed: 05/22/2018

NOTICE OF ACCEPTANCE OF APPLICATION UNDER 35 U.S.C 371 AND 37 CFR 1.495

The applicant is hereby advised that the United States Patent and Trademark Office, in its capacity as a Designated / Elected Office (37 CFR 1.495), has ACCEPTED the above identified international application for national patentability examination in the United States Patent and Trademark Office.

The United States Application Number assigned to the application is shown above. A Filing Receipt will be issued for the present application in due course. **THE DATE APPEARING ON THE FILING RECEIPT AS THE "FILING DATE or 371(c) DATE" IS THE DATE ON WHICH THE LAST OF THE 35 U.S.C. 371 (c)(1) and (c)(2) REQUIREMENTS HAS BEEN RECEIVED IN THE OFFICE. THIS DATE IS SHOWN BELOW.** The filing date of the above identified application is the international filing date of the international application (Article 11(3) and 35 U.S.C. 363)

02/14/2018
DATE OF RECEIPT OF 35 U.S.C.
371(c)(1) and (c)(2) REQUIREMENTS

The following items have been received:

- Indication of Small Entity Status
- Copy of the International Application filed on 02/14/2018
- Copy of the International Search Report filed on 02/14/2018
- Preliminary Amendments filed on 02/14/2018
- Information Disclosure Statements filed on 02/14/2018
- Inventor's Oath or Declaration filed on 02/26/2018
- U.S. Basic National Fees filed on 02/14/2018
- Authorize Access to Search Results filed on 02/14/2018
- Priority Documents filed on 02/14/2018
- Power of Attorney filed on 02/26/2018
- Specification filed on 02/14/2018
- Claims filed on 02/14/2018
- Abstracts filed on 02/14/2018
- Drawings filed on 02/14/2018
- Authorization to Permit Access filed on 02/14/2018
- Application Data Sheet (37 CFR 1.76) filed on 02/14/2018

Applicant is reminded that any communications to the United States Patent and Trademark Office must be mailed to the address given in the heading and include the U.S. application no. shown above (37 CFR 1.5)

BRIAN A HARDEN

Telephone: (703) 756-1815

JPMC Ex. 1002
Page 349

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
15/752,711	02/14/2018		1060	AMK-5243-9	20	3

CONFIRMATION NO. 5327

FILING RECEIPT

23117
NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203



Date Mailed: 05/22/2018

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Nick Armstrong, Sydney, AUSTRALIA;
Ben Buckingham, Sydney, AUSTRALIA;
Daniel Friedman, Sydney, AUSTRALIA;
Elliot Shepherd, Sydney, AUSTRALIA;
Eric Knight, Sydney, AUSTRALIA;

Applicant(s)

Identitii Pty Ltd, Surry Hills, New South Wales, AUSTRALIA;

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a 371 of PCT/AU2016/000279 08/12/2016

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.)
AUSTRALIA 2015903292 08/14/2015
AUSTRALIA 2016901924 05/20/2016
AUSTRALIA 2016900239 01/27/2016

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 05/21/2018

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 15/752,711**

Projected Publication Date: 08/30/2018

Non-Publication Request: No

Early Publication Request: No
**** SMALL ENTITY ****
Title

COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR

Preliminary Class

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 15/752,711

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	150		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	260		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	380		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	20 minus 20 =	*	x 50 =	0.00	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*	x 230 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			200			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	990		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

Doc Code: PA
Document Description: Power of Attorney

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	15/752,711
Filing Date	02/14/2018
First Named Inventor	ARMSTRONG, Nick
Title	COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR
Art Unit	Not Yet Assigned
Examiner Name	Not Yet Assigned
Attorney Docket Number	AMK-5243-0009

SIGNATURE of Applicant or Patent Practitioner

Signature	/Alan M. Kagen/	Date (Optional)	February 26, 2018
Name	Alan M. Kagen	Registration Number	36,178
Title (if Applicant is a juristic entity)			
Applicant Name (if Applicant is a juristic entity)			

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

*Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Doc Code: PA
Document Description: Power of Attorney

GENERAL POWER OF ATTORNEY BY APPLICANT

(ASSIGNEE, LEGAL REPRESENTATIVE OR PERSON WHO OTHERWISE SHOWS SUFFICIENT PROPRIETARY INTEREST)

I hereby revoke all previous powers of attorney given in the application identified in the attached Transmittal for Power of Attorney form.

I hereby appoint Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A or equivalent)

23117

Please recognize or change the correspondence address for the application identified in the attached transmittal letter (form PTO/AIA/82A or equivalent to the address associated with the above-mentioned Customer Number.

I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

Identitii Pty Ltd

☐ Inventor or Joint Inventor (title not required below)

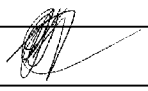
☐ Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)

☒ Assignee or Person to Whom the Inventor is Under an Obligation to Assign and am authorized to act on behalf of all assignees (provide signer's title if applicant is a juristic entity)

☐ Person Who Otherwise Shows Sufficient *Proprietary* Interest (*e.g.*, a petition under 37 CFR 1.46 (b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity)

Signature		Date	02/26/2018
Name	Nicholas Armstrong		
Title	CEO & Managing Director		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

Total of 1 forms are submitted.

JPMC Ex. 1002
Doc ID: 0844398da00b51155155271f9c8b468276e623ea

Electronic Acknowledgement Receipt

EFS ID:	31882029
Application Number:	15752711
International Application Number:	
Confirmation Number:	5327
Title of Invention:	COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR
First Named Inventor/Applicant Name:	Nick Armstrong
Customer Number:	23117
Filer:	Alan Mark Kagen/Janet Stoy
Filer Authorized By:	Alan Mark Kagen
Attorney Docket Number:	AMK-5243-9
Receipt Date:	26-FEB-2018
Filing Date:	
Time Stamp:	11:26:23
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	5243-9_submit_combo_dec_and_asn_and_power_by_applicant.pdf	43722 e7198afe994e20b11a6927cef5a6cf4fa2cd3c22	no	3

Warnings:

Information:					
2	Power of Attorney	5243-9_power_by_applicant.pdf	419460 30374cf223a832184be1fdf4bd26cc41012386af	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	463182		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

	U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTORNEY DOCKET NUMBER AMK-5243-0009
TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371		U.S. APPLICATION NO. (If known, see 37 C.F.R. 1.5) 15/752,711
INTERNATIONAL APPLICATION NO. PCT/AU2016/000279	INTERNATIONAL FILING DATE 08/12/2016	PRIORITY DATE CLAIMED 08/14/2015
TITLE OF INVENTION		CONFIRMATION NO.: 5327
COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR		
FIRST NAMED INVENTOR		
ARMSTRONG, Nick		

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☐ This is a **FIRST** submission of items concerning a submission under 35 U.S.C. 371.
2. ☒ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a submission under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). NOTE: The express request under 35 U.S.C. 371(f) will not be effective unless the requirements under 35 U.S.C. 371(c)(1), (2), and (4) for payment of the basic national fee, copy of the International Application and English translation thereof (if required), and/or the oath or declaration of the inventor(s) have been received.
4. A copy of the International Application as filed (35 U.S.C. 371(c)(2):
   a. ☐ WO 2017/027900 A1 is attached (pages specification, claims & abstract (claims), sheets drawings).
   b. ☐ has been communicated by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
5. An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)):
   a. ☐ is attached (pages specification, claims & abstract (claims), sheets drawings, page Certificate of Translation).
   b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
6. An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4):
   a. ☒ is attached. (Combined Declaration and Assignment filed through EPAS)
   b. ☐ was previously submitted to the International Bureau during the international phase under PCT Rule 4.17(iv).

Items 7 to 10 below concern amendments made in the international phase

PCT Article 19 and 34 Amendments

7. ☐ Amendments to the claims of the International Application under PCT Article 19 are attached (required only if not communicated by the International Bureau). (35 U.S.C. 371(c)(3).
8. ☐ English language translation of the amendments to the claims under PCT Article 19 is attached (35 U.S.C. 371(c)(3).
9. ☐ English language translation of the annexes (article 19 and/or 34 amendments only) of the International Preliminary Examination Report is attached (35 U.S.C. 371(c)(5).

Cancellation of Amendments Made in the International Phase

10. Do not enter the amendment made in the international phase:
    a. ☐ under PCT Article 19. ☐ under PCT Article 34.

NOTE: A proper amendment made in English under Article 19 or 34 will be entered in the U.S. national phase application absent a clear instruction from applicant not to enter the amendment(s)

Items 11 to 18 below concern document(s) or information included.

11. ☐ An Information Disclosure Statement under 37 C.F.R. 1.97 and 1.98.
12. ☐ A Preliminary Amendment.
13. ☐ An Application Data Sheet under 37 C.F.R. § 1.76.
14. ☐ A substitute specification. NOTE: A substitute specification cannot include claims. See 37 CFR 1.125(b).
15. ☒ A Power of Attorney and/or change of address letter. ☐ 37 CFR 3.73(c) Statement (when there is an Assignee).
16. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13*ter*.3 and 37 CFR 1.821-1.825.
17. ☐ An assignment document for recording (cover sheet and document(s) if paper filing). Name of Assignee: Identitii Pty Ltd
18. ☐ Other items or information.

Mail Stop PCT

U.S. APPLN. NO. (If known, see 37 CFR 1.5)	INTERNATIONAL APPLICATION NO. PCT/AU2016/000279	ATTORNEY'S DOCKET NUMBER AMK-5243-0009

☐ The following fees are submitted:		CALCULATIONS	PTO USE ONLY
	BASIC NATIONAL FEE (37 C.F.R. 1.492(a):		
19. ☐	Basic national fee..... $300.00 (1631)/$150.00 (2631)/$75.00 (3631) PLUS SURCHARGE **IF** Paper Filing (EFF. 11.15.2011)$400.00 (1690)/$200.00 (2690)//$200.00 (3690)	$	
20. ☐	Examination Fee..... $ $760.00 (1633)/$380.00 (2633)/$190.00 (3633)	$	
21. ☐	Search Fee .....$ ..... $140.00 (1641)/$70.00 (2641)/$35.00 (3641) ..... $520.00 (1642)/$260.00 (2642)/$130.00 (3642) ..... $660.00 (1632)/$330.00 (2632)/$165.00 (3632)	$	
	TOTAL OF ABOVE CALCULATIONS	$ **0.00**	
☐	Additional fee for specification and drawings filed in paper over 100 sheets (excluding sequence listing or computer program listing filed in an electronic medium). The fee is $400.00 (1681)/$200.00 (2681)/$100.00 (3681) for each additional 50 sheets of paper or fraction thereof.		

Total Sheets	Extra Sheets	Number of each additional 50 or fraction thereof (round **up** to a whole number)	RATE		
-100 =	0 /50 =	0.00		$**0.00** (1681) $**0.00** (2681) $**0.00** (3681)	$

Surcharge of **$140.00 (1617)/$70.00 (2617)/$35.00 (3617)** for furnishing any of the search fee, examination fee, or the oath or declaration later than ☐ 30 months from the earliest claimed priority date (37 C.F.R. 1.492(h).	$	

CLAIMS	NUMBER FILED		# EXTRA	RATE			
Total Claims		minus 20 =	0 X	$100.00 (1615)/$50.00 (2615)/$25.00 (3615) $460.00 (1614)/$230.00 (2614)/$115.00 (3614)		$	
Independent Claims		minus 3 =	0 X			$	
MULTIPLE DEPENDENT CLAIMS(S) (if applicable)				$780.00 (1616)/$390.00 (2616)/$195.00 (3616)		$	

Petition is hereby made to extend the current due date so as to cover the filing date of this paper and attachment(s): One Month Extension $200.00 (1251)/$100.00 (2251)/$50.00 (3251); Two Month Extension $600.00 (1252)/$300.00 (2252)/$150.00 (3252); Three Month Extension $1400.00 (1253)/$700.00 (2253)/$350.00 (3253); Four Month Extension $2200.00 (1254)/$1100.00 (2254)/$550.00 (3254); Five Month Extensions $3000.00 (1255)/$1500.00 (2255)/$750.00 (3255)	$	
☒ Applicant claims small entity status. See 37 CFR 1.27. ☐ Applicant claims "micro entity" status. See 37 CFR 1.29 ☐ Micro entity certification statement filed herewith		
Processing fee of **$140.00 (1618)/$70.00 (2618)/$35.00 (3618)**, for furnishing the English Translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 C.F.R. 1.492(i).		
TOTAL NATIONAL FEE =	$ **0.00**	
Fee for recording the enclosed assignment (37 C.F.R. 1.21(h). The assignment must be accompanied by an appropriate cover sheet (37 C.F.R. 3.28, 3.31). **$50.00** (8021) /**$0 if filed electronically** per property	$	
Fee for Petition to Revive Unintentionally Abandoned Application;$ **2000.00(1453)/1000.00(2453)/500.00(3453)**	$	
TOTAL FEES ENCLOSED =	$ **0.00**	
	Amount to be refunded: $	
	Amount to be Charged: $	

a. ☐ CREDIT CARD OR DEPOSIT ACCOUNT PAYMENT (CREDIT CARD FORM ATTACHED IF PAPER FILING).

b. ☐ Please charge my Deposit Account No. 14-1140 in the amount of $_____ to cover the above fees.

c. ☒ The Commissioner is hereby authorized to charge any deficiency, or credit any overpayment, in the fee(s) filed, or asserted to be filed, or which should have been filed herewith (or with any paper hereafter filed in this application by this firm) to Deposit Account No. 14-1140. **However, authorization is NOT given hereby to charge any extra claims fee or multiple dependent claims fees.**

d. ☐ The entire content of International Application No. PCT/AU2016/000279 and any U.S. and foreign application(s) corresponding thereto, and AU 2015903292; AU 2016900239; and AU 2016901924, referred to in this application is/are hereby incorporated by reference in this application.

NOTE: Where an appropriate time limit under 37 C.F.R. 1.494 or 1.495 has not been met, a petition to revive (37 C.F.R. 1.137(a) or (b) must be filed and granted to restore the application to pending status.

Mail Stop PCT

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File)Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013, and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.

NOTE: A U.S. national stage application may not claim priority to the international application of which it is the national phase. The filing date of a U.S. national stage application is the international filing date. See 35 U.S.C. 363

CORRESPONDENCE ADDRESS

Direct all correspondence to:

☒ **Customer Number:** **23117**

Type Customer Number here

Telephone: (703) 816-4000

AMK: jls

/Alan M. Kagen/

Alan M. Kagen

NAME

36,178

REGISTRATION NUMBER

February 26, 2018

Date

PATENT ASSIGNMENT COVER SHEET

Electronic Version v1.1
Stylesheet Version v1.2

EPAS ID: PAT4839399

SUBMISSION TYPE:	NEW ASSIGNMENT
NATURE OF CONVEYANCE:	ASSIGNMENT

CONVEYING PARTY DATA

Name	Execution Date
NICK ARMSTRONG	02/26/2018
BEN BUCKINGHAM	02/22/2018
DANIEL FRIEDMAN	02/23/2018
ELLIOT SHEPHERD	02/22/2018
ERIC KNIGHT	02/22/2018

RECEIVING PARTY DATA

Name:	IDENTITII PTY LTD
Street Address:	SUITE 1 LEVEL 3, 66-72 RESERVOIR ST.
City:	SURRY HILLS, NEW SOUTH WALES
State/Country:	AUSTRALIA
Postal Code:	2010

PROPERTY NUMBERS Total: 1

Property Type	Number
Application Number:	15752711

CORRESPONDENCE DATA

Fax Number: (703)816-4100

Correspondence will be sent to the e-mail address first; if that is unsuccessful, it will be sent using a fax number, if provided; if that is unsuccessful, it will be sent via US Mail.

Phone: 703-816-4000
Email: PTOMAIL@nixonvan.com
Correspondent Name: ALAN M. KAGEN/NIXON & VANDERHYE, PC
Address Line 1: 901 NORTH GLEBE ROAD, 11TH FLOOR
Address Line 4: ARLINGTON, VIRGINIA 22203

ATTORNEY DOCKET NUMBER:	AMK-5243-9
NAME OF SUBMITTER:	ALAN M. KAGEN
SIGNATURE:	/Alan M. Kagen/
DATE SIGNED:	02/26/2018
	This document serves as an Oath/Declaration (37 CFR 1.63).

Total Attachments: 5

source=5243-9_combo_dec_and_asn#page1.tif
source=5243-9_combo_dec_and_asn#page2.tif
source=5243-9_combo_dec_and_asn#page3.tif
source=5243-9_combo_dec_and_asn#page4.tif
source=5243-9_combo_dec_and_asn#page5.tif

Doc code: Oath
Document Description: Oath or declaration filed

Attorney Docket Number	AMK-5243-0009
First Named Inventor	ARMSTRONG, Nick

INVENTOR'S DECLARATION AND ASSIGNMENT FOR UTILITY OR DESIGN PATENT APPLICATION (37 CFR 1.63) USING AN APPLICATION DATA SHEET (37 CFR 1.76)

☐ Declaration Submitted With Initial Filing
OR
☒ Declaration Submitted After Initial Filing (surcharge (37 C.F.R. § 1.16(f)) required)

COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR

(Title of the Invention)

As a below named inventor, I hereby declare that:

This declaration is directed to:
☐ the attached application, or
☒ United States Application Number 15/752,711 filed February 14, 2018, or
☐ PCT International application number filed on .

The above-identified application was made or authorized to be made by me.

I believe I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WHEREAS, the undersigned (hereinafter ASSIGNOR), has made an invention in the Application identified above.

WHEREAS, Identitii Pty Ltd (hereinafter ASSIGNEE), an entity, having an office and place of business at Suite 1 Level 3, 66-72 Reservoir St., Surry Hills, New South Wales, Australia 2010, is desirous of acquiring an interest therein;

NOW, THEREFORE, in consideration of Ten Dollars ($10.00) and/or other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the said ASSIGNOR by these presents hereby sells, assigns, and transfers unto the said ASSIGNEE, its successors, assigns, and legal representatives, ASSIGNOR'S entire right, title and interest in the United States of America and all foreign countries, in and to the invention as described in the aforesaid application, and to the said application and to all subsequent applications based thereon including any and all continuations, divisions, reissues, and substitutes of said application, and all resulting patents, together with the right of priority under the International Convention for the Protection of Industrial Property, Inter-American Convention Relating to Patents, Designs and Industrial Models, and any other international agreements to which the United States of America adheres, and the ASSIGNOR hereby authorizes and requests the Commissioner of Patents and Trademarks to issue said Letters Patent to ASSIGNEE, for its interest as ASSIGNEE, its successors, assigns, and legal representatives. It is understood and agreed that ASSIGNEE'S attorneys Nixon & Vanderhye P.C. have represented only ASSIGNEE and will continue to represent only ASSIGNEE with respect to this invention;

ASSIGNOR hereby agrees to transfer a like interest upon request of said ASSIGNEE, its successors, assigns, and legal representatives, and without further remuneration, in and to any improvements, and applications for patents based thereon, growing out of or related to the said invention;

ASSIGNOR hereby agrees to execute any papers by ASSIGNEE, its successors, assigns, and legal representatives, deemed essential to ASSIGNEE'S full protection and title in and to the invention hereby transferred; and

ASSIGNOR hereby agrees, upon request of ASSIGNEE, and without further remuneration, to execute any and all papers desired by ASSIGNEE, for the filing and granting of foreign applications and the perfecting of title thereto in ASSIGNEE.

AGREED and executed as noted below:

LEGAL NAME OF INVENTOR/JOINT INVENTOR:	
(E.g., Given Name (first and middle (if any)) and Family Name or Surname)	
Nick	ARMSTRONG
Inventor's Signature: 	Date: 02/26/2018
Witnessed by: Name: Benjamin Buckingham	
Signature of witness: 	Date: 02/22/2018

I/We acknowledge the duty to disclose information which is material to the patentability of this application as defined in 37 CFR §1.56.

Doc code: Oath
Document Description: Oath or declaration filed

Attorney Docket Number	AMK-5243-0009
First Named Inventor	ARMSTRONG, Nick

INVENTOR'S DECLARATION AND ASSIGNMENT FOR UTILITY OR DESIGN PATENT APPLICATION (37 CFR 1.63) USING AN APPLICATION DATA SHEET (37 CFR 1.76)

☐ Declaration Submitted With Initial Filing

OR

☒ Declaration Submitted After Initial Filing (surcharge (37 C.F.R. § 1.16(f)) required)

COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR

(Title of the Invention)

As a below named inventor, I hereby declare that:

This declaration is directed to:

☐ the attached application, or

☒ United States Application Number 15/752,711 filed February 14, 2018, or

☐ PCT International application number filed on .

The above-identified application was made or authorized to be made by me.

I believe I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WHEREAS, the undersigned (hereinafter ASSIGNOR), has made an invention in the Application identified above.

WHEREAS, Identitii Pty Ltd (hereinafter ASSIGNEE), an entity, having an office and place of business at Suite 1 Level 3, 66-72 Reservoir St., Surry Hills, New South Wales, Australia 2010, is desirous of acquiring an interest therein;

NOW, THEREFORE, in consideration of Ten Dollars ($10.00) and/or other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the said ASSIGNOR by these presents hereby sells, assigns, and transfers unto the said ASSIGNEE, its successors, assigns, and legal representatives, ASSIGNOR'S entire right, title and interest in the United States of America and all foreign countries, in and to the invention as described in the aforesaid application, and to the said application and to all subsequent applications based thereon including any and all continuations, divisions, reissues, and substitutes of said application, and all resulting patents, together with the right of priority under the International Convention for the Protection of Industrial Property, Inter-American Convention Relating to Patents, Designs and Industrial Models, and any other international agreements to which the United States of America adheres, and the ASSIGNOR hereby authorizes and requests the Commissioner of Patents and Trademarks to issue said Letters Patent to ASSIGNEE, for its interest as ASSIGNEE, its successors, assigns, and legal representatives. It is understood and agreed that ASSIGNEE'S attorneys Nixon & Vanderhye P.C. have represented only ASSIGNEE and will continue to represent only ASSIGNEE with respect to this invention;

ASSIGNOR hereby agrees to transfer a like interest upon request of said ASSIGNEE, its successors, assigns, and legal representatives, and without further remuneration, in and to any improvements, and applications for patents based thereon, growing out of or related to the said invention;

ASSIGNOR hereby agrees to execute any papers by ASSIGNEE, its successors, assigns, and legal representatives, deemed essential to ASSIGNEE'S full protection and title in and to the invention hereby transferred; and

ASSIGNOR hereby agrees, upon request of ASSIGNEE, and without further remuneration, to execute any and all papers desired by ASSIGNEE, for the filing and granting of foreign applications and the perfecting of title thereto in ASSIGNEE.

AGREED and executed as noted below:

Legal Name of Additional Joint Inventor, if any:	
(E.g., Given Name (first and middle (if any)) and Family Name or Surname)	
Ben	BUCKINGHAM
Inventor's Signature:	Date: 02/22/2018
Witnessed by: Name: Nicholas Armstrong	
Signature of witness:	Date: 02/26/2018

I/We acknowledge the duty to disclose information which is material to the patentability of this application as defined in 37 CFR §1.56.

Doc code: Oath
Document Description: Oath or declaration filed

Attorney Docket Number	AMK-5243-0009
First Named Inventor	ARMSTRONG, Nick

INVENTOR'S DECLARATION AND ASSIGNMENT FOR UTILITY OR DESIGN PATENT APPLICATION (37 CFR 1.63) USING AN APPLICATION DATA SHEET (37 CFR 1.76)

☐ Declaration Submitted With Initial Filing
OR
☒ Declaration Submitted After Initial Filing (surcharge (37 C.F.R. § 1.16(f)) required)

COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR

(Title of the Invention)

As a below named inventor, I hereby declare that:

This declaration is directed to:
☐ the attached application, or
☒ United States Application Number 15/752,711 filed February 14, 2018, or
☐ PCT International application number filed on .

The above-identified application was made or authorized to be made by me.

I believe I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WHEREAS, the undersigned (hereinafter ASSIGNOR), has made an invention in the Application identified above.

WHEREAS, Identitii Pty Ltd (hereinafter ASSIGNEE), an entity, having an office and place of business at Suite 1 Level 3, 66-72 Reservoir St., Surry Hills, New South Wales, Australia 2010, is desirous of acquiring an interest therein;

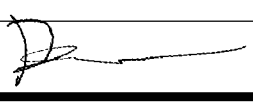
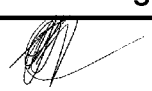
NOW, THEREFORE, in consideration of Ten Dollars ($10.00) and/or other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the said ASSIGNOR by these presents hereby sells, assigns, and transfers unto the said ASSIGNEE, its successors, assigns, and legal representatives, ASSIGNOR'S entire right, title and interest in the United States of America and all foreign countries, in and to the invention as described in the aforesaid application, and to the said application and to all subsequent applications based thereon including any and all continuations, divisions, reissues, and substitutes of said application, and all resulting patents, together with the right of priority under the International Convention for the Protection of Industrial Property, Inter-American Convention Relating to Patents, Designs and Industrial Models, and any other international agreements to which the United States of America adheres, and the ASSIGNOR hereby authorizes and requests the Commissioner of Patents and Trademarks to issue said Letters Patent to ASSIGNEE, for its interest as ASSIGNEE, its successors, assigns, and legal representatives. It is understood and agreed that ASSIGNEE'S attorneys Nixon & Vanderhye P.C. have represented only ASSIGNEE and will continue to represent only ASSIGNEE with respect to this invention;

ASSIGNOR hereby agrees to transfer a like interest upon request of said ASSIGNEE, its successors, assigns, and legal representatives, and without further remuneration, in and to any improvements, and applications for patents based thereon, growing out of or related to the said invention;

ASSIGNOR hereby agrees to execute any papers by ASSIGNEE, its successors, assigns, and legal representatives, deemed essential to ASSIGNEE'S full protection and title in and to the invention hereby transferred; and

ASSIGNOR hereby agrees, upon request of ASSIGNEE, and without further remuneration, to execute any and all papers desired by ASSIGNEE, for the filing and granting of foreign applications and the perfecting of title thereto in ASSIGNEE.

AGREED and executed as noted below:

Legal Name of Additional Joint Inventor, if any:	
(E.g., Given Name (first and middle (if any)) and Family Name or Surname)	
Daniel	FRIEDMAN
Inventor's Signature: 	Date: 02/23/2018
Witnessed by: Name: Nicholas Armstrong	
Signature of witness: 	Date: 02/26/2018

I/We acknowledge the duty to disclose information which is material to the patentability of this application as defined in 37 CFR §1.56.

Doc code: Oath
Document Description: Oath or declaration filed

Attorney Docket Number	AMK-5243-0009
First Named Inventor	ARMSTRONG, Nick

INVENTOR'S DECLARATION AND ASSIGNMENT FOR UTILITY OR DESIGN PATENT APPLICATION (37 CFR 1.63) USING AN APPLICATION DATA SHEET (37 CFR 1.76)

☐ Declaration Submitted With Initial Filing
OR
☒ Declaration Submitted After Initial Filing (surcharge (37 C.F.R. § 1.16(f)) required)

COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR

(Title of the Invention)

As a below named inventor, I hereby declare that:

This declaration is directed to:
☐ the attached application, or
☒ United States Application Number 15/752,711 filed February 14, 2018, or
☐ PCT International application number filed on .

The above-identified application was made or authorized to be made by me.

I believe I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WHEREAS, the undersigned (hereinafter ASSIGNOR), has made an invention in the Application identified above.

WHEREAS, Identitii Pty Ltd (hereinafter ASSIGNEE), an entity, having an office and place of business at Suite 1 Level 3, 66-72 Reservoir St., Surry Hills, New South Wales, Australia 2010, is desirous of acquiring an interest therein;

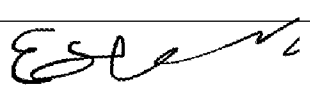
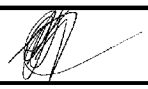
NOW, THEREFORE, in consideration of Ten Dollars ($10.00) and/or other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the said ASSIGNOR by these presents hereby sells, assigns, and transfers unto the said ASSIGNEE, its successors, assigns, and legal representatives, ASSIGNOR'S entire right, title and interest in the United States of America and all foreign countries, in and to the invention as described in the aforesaid application, and to the said application and to all subsequent applications based thereon including any and all continuations, divisions, reissues, and substitutes of said application, and all resulting patents, together with the right of priority under the International Convention for the Protection of Industrial Property, Inter-American Convention Relating to Patents, Designs and Industrial Models, and any other international agreements to which the United States of America adheres, and the ASSIGNOR hereby authorizes and requests the Commissioner of Patents and Trademarks to issue said Letters Patent to ASSIGNEE, for its interest as ASSIGNEE, its successors, assigns, and legal representatives. It is understood and agreed that ASSIGNEE'S attorneys Nixon & Vanderhye P.C. have represented only ASSIGNEE and will continue to represent only ASSIGNEE with respect to this invention;

ASSIGNOR hereby agrees to transfer a like interest upon request of said ASSIGNEE, its successors, assigns, and legal representatives, and without further remuneration, in and to any improvements, and applications for patents based thereon, growing out of or related to the said invention;

ASSIGNOR hereby agrees to execute any papers by ASSIGNEE, its successors, assigns, and legal representatives, deemed essential to ASSIGNEE'S full protection and title in and to the invention hereby transferred; and

ASSIGNOR hereby agrees, upon request of ASSIGNEE, and without further remuneration, to execute any and all papers desired by ASSIGNEE, for the filing and granting of foreign applications and the perfecting of title thereto in ASSIGNEE.

AGREED and executed as noted below:

Legal Name of Additional Joint Inventor, if any:	
(E.g., Given Name (first and middle (if any)) and Family Name or Surname)	
Elliot	SHEPHERD
Inventor's Signature: 	Date: 02/22/2018
Witnessed by: Name: Nicholas Armstrong	
Signature of witness: 	Date: 02/26/2018

I/We acknowledge the duty to disclose information which is material to the patentability of this application as defined in 37 CFR §1.56.

Doc code: Oath
Document Description: Oath or declaration filed

Attorney Docket Number	AMK-5243-0009
First Named Inventor	ARMSTRONG, Nick

INVENTOR'S DECLARATION AND ASSIGNMENT FOR UTILITY OR DESIGN PATENT APPLICATION (37 CFR 1.63) USING AN APPLICATION DATA SHEET (37 CFR 1.76)

☐ Declaration Submitted With Initial Filing

OR

☒ Declaration Submitted After Initial Filing (surcharge (37 C.F.R. § 1.16(f)) required)

COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR

(Title of the Invention)

As a below named inventor, I hereby declare that:

This declaration is directed to:

☐ the attached application, or

☒ United States Application Number 15/752,711 filed February 14, 2018, or

☐ PCT International application number filed on .

The above-identified application was made or authorized to be made by me.

I believe I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WHEREAS, the undersigned (hereinafter ASSIGNOR), has made an invention in the Application identified above.

WHEREAS, Identitii Pty Ltd (hereinafter ASSIGNEE), an entity, having an office and place of business at Suite 1 Level 3, 66-72 Reservoir St., Surry Hills, New South Wales, Australia 2010, is desirous of acquiring an interest therein;

NOW, THEREFORE, in consideration of Ten Dollars ($10.00) and/or other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the said ASSIGNOR by these presents hereby sells, assigns, and transfers unto the said ASSIGNEE, its successors, assigns, and legal representatives, ASSIGNOR'S entire right, title and interest in the United States of America and all foreign countries, in and to the invention as described in the aforesaid application, and to the said application and to all subsequent applications based thereon including any and all continuations, divisions, reissues, and substitutes of said application, and all resulting patents, together with the right of priority under the International Convention for the Protection of Industrial Property, Inter-American Convention Relating to Patents, Designs and Industrial Models, and any other international agreements to which the United States of America adheres, and the ASSIGNOR hereby authorizes and requests the Commissioner of Patents and Trademarks to issue said Letters Patent to ASSIGNEE, for its interest as ASSIGNEE, its successors, assigns, and legal representatives. It is understood and agreed that ASSIGNEE'S attorneys Nixon & Vanderhye P.C. have represented only ASSIGNEE and will continue to represent only ASSIGNEE with respect to this invention;

ASSIGNOR hereby agrees to transfer a like interest upon request of said ASSIGNEE, its successors, assigns, and legal representatives, and without further remuneration, in and to any improvements, and applications for patents based thereon, growing out of or related to the said invention;

ASSIGNOR hereby agrees to execute any papers by ASSIGNEE, its successors, assigns, and legal representatives, deemed essential to ASSIGNEE'S full protection and title in and to the invention hereby transferred; and

ASSIGNOR hereby agrees, upon request of ASSIGNEE, and without further remuneration, to execute any and all papers desired by ASSIGNEE, for the filing and granting of foreign applications and the perfecting of title thereto in ASSIGNEE.

AGREED and executed as noted below:

Legal Name of Additional Joint Inventor, if any:	
(E.g., Given Name (first and middle (if any)) and Family Name or Surname)	
Eric	KNIGHT
Inventor's Signature: Eric Knight	Date: 02/22/2018
Witnessed by: Name: Nicholas Armstrong	
Signature of witness:	Date: 02/26/2018

I/We acknowledge the duty to disclose information which is material to the patentability of this application as defined in 37 CFR §1.56.

Australian Government

PCT/AU2016/000279

Patent Office
Canberra

I, VIVIENNE IGLESIAS, DELEGATE OF THE COMMISSIONER, hereby certify that annexed is a true copy of the Provisional specification in connection with Application No. 2015903292 for a patent by SPARRO (AUSTRALIA) PTY LTD as filed on 14 August 2015.

WITNESS my hand this
THIRTEENTH day of September 2016

VIVIENNE IGLESIAS
DELEGATE OF THE COMMISSIONER

COMMONWEALTH OF AUSTRALIA
AUSTRALIA
PATENT OFFICE

14 Aug 2015 2015903292

Payment Messaging System

TECHNICAL FIELD

[0001] The present invention relates to settlement systems and, more particularly although not exclusively, to a payment messaging system particularly, although not exclusively, suited to electronic transactions.

BACKGROUND

[0002] "Settlement" in the sense of settling amounts owing as between two parties, whether in a Fiat currency or in the newer forms of electronic currency (such as "Bitcoin") is a known concept which is central to the workings of most financial systems. In the case of electronic currency which requires settlement by exchange of data between institutions the current system is quite cumbersome and leads to many costs due in part to the necessity for often repeated data entry of significant amounts of data into systems run by the parties to any given transaction requiring settlement and also to the intermediaries that it almost every instance (barring a non-electronic cash transaction) form part of a chain of intermediaries that become involved in ultimately effecting settlement of any given transaction.

[0003] In particular implementations of settlement systems across the internet, a block chain structure may be utilised where a block chain is a distributed database that maintains a continuously growing list of data records that may be hardened against tampering and revision. The most widely known application of a block chain is the public ledger of transactions for cryptocurrencies, such as Bitcoin referenced above.

[0004] Many settlement systems are characterised by effectively one-way transmission of data in any given data exchange transaction (for example systems based on Swift messaging). If it is subsequently discovered that there are deficiencies in the data thus transmitted there can then ensue time consuming checking and querying operations before settlement can be effected.

[0005] It is an object of the present invention to address or at least ameliorate some of the above disadvantages.

Notes

[0006] The term "comprising" (and grammatical variations thereof) is used in this specification in the inclusive sense of "having" or "including", and not in the exclusive sense of "consisting only of".

2015903292 14 Aug 2015

[0007] The above discussion of the prior art in the Background of the invention, is not an admission that any information discussed therein is citable prior art or part of the common general knowledge of persons skilled in the art in any country.

SUMMARY OF INVENTION

Definitions:

[0008] **token:** in this specification a "token" is a data record containing data required to settle a transaction for which the token has been generated; and wherein the data is rendered, formatted or passed through an algorithm in a predetermined manner. The process of rendering, formatting or passing through an algorithm in a predetermined manner is termed "tokenisation". The tokenisation process may involve operations such as encryption and de-identification of data.

[0009] **Transaction:** in this specification "transaction" refers to a trade between two parties, for example at least a first transacting entity and a second transacting entity and wherein the trade is expressed in a financial form (for example in a Fiat currency or an electronic currency-to be distinguished, for example, from a barter transaction) which will ultimately require exchange of currency to settle the transaction. In some instances the currency will be the same on both sides of the transaction. In other cases a conversion from one currency to another may be required.

[00010] Accordingly, in one broad form of the invention, there is provided a system for settling a transaction electronically; said system comprising:

at least a first transacting entity;

at least a second transacting entity;

at least a first intermediary entity;

at least a second intermediary entity;

in the case where the first transacting entity enters into a transaction with the second transacting entity generating a tokenised message at the time of the transaction containing data needed to settle the transaction;

initiating settlement of the transaction by transmission of the tokenised message to the at least first transacting entity.

[00011] In a further broad form of the invention there is provided a tokenised message construction system; said system comprising:

a server in communication with a database and which facilitates communications between a plurality of parties to a transaction;

2015903292 14 Aug 2015

each party having a digitised device with which to communicate with other ones of the parties and with the server;

each party capable of generating a tokenised message via a bidirectional communication with the server.

[00012] Preferably the tokenised message is generated with reference to a token database located at a remote location.

[00013] Preferably the tokenised message includes at least a first data element, a second data element and a third data element.

[00014] Preferably the first data element comprises identification data for a payor, the second data element comprises identification data for a payee (biller) and the third data element comprises identification currency, denomination and value data.

[00015] Preferably a further tokenised message is generated by either an intermediary entity or the token database.

[00016] Preferably a tokenised message is generated by a bi-directional communication process.

[00017] Preferably the bi-directional communication process is between the token database and an intermediary entity.

[00018] Preferably a step in producing a tokenised message involves de-identifying data.

[00019] Preferably a step in producing a tokenised message involves adding a data element to the message.

[00020] Preferably a step in producing a tokenised message involves removing a data element from the message.

[00021] Preferably a step in producing a tokenised message involves applying an algorithm to the data elements in the message.

[00022] Preferably the token database sequences the tokenised messages.

[00023] Preferably the token database sequences the tokenised messages and transmits the tokenised messages as payment data records to a block chain settlement system.

[00024] Preferably the block chain settlement system employs the Ripple protocol.

BRIEF DESCRIPTION OF DRAWINGS

[00025] Embodiments of the present invention will now be described with reference to the accompanying drawings wherein:

2015903292 14 Aug 2015

[00026] Figure 1A is a block diagram of the entities and intermediaries involved in a prior art electronic settlement system;

[00027] Figure 1B is a data and funds flow according to a prior art settlement system;

[00028] Figure 2A is a data and funds flow diagram according to an indicative embodiment of the present invention;

[00029] Figure *2C* is a block diagram of the basic infrastructure and components suited for use with embodiments of the present invention and

[00030] Figure 3 A, B, C comprise block diagrams of the steps in a settlement transaction in accordance with a first preferred embodiment of the present invention

0031] Figure 4 is a block diagram of salient characteristics of a messaging system 10 of the prior art as compared with the salient messaging characteristics of the system 210 enabled by the code of a second embodiment.

0032] Figure 5 illustrates the options for data content to be included in tokens in accordance with embodiments of the invention as described above.

0033] Figure 6 provides a comparison of characteristics of embodiments of the present invention as compared with the prior art Swift-based messaging system.

[00034]

DESCRIPTION OF EMBODIMENTS

[00035] With reference to Figure 1 there is illustrated in block form the basic components of a prior art settlement system. In many transactions there will be an at least first transacting entity 11 which enters into a transaction with an at least second transacting entity 12. The transaction may be as simple as the agreement by the first transacting entity 11 to sell a particular item or service to the second transacting entity 12. Typically the transaction will require settlement for an agreed amount expressed in a Fiat or other currency. In the vast majority of cases the at least first transacting entity 11 will be associated with an at least first intermediary entity 13, in this instance in the form of a bank A and similarly the second transacting entity 12 will be associated with an at least second

2015903292 14 Aug 2015

intermediary entity 14 in this instance in the form of bank B. The first transacting entity 11 will have a first bank account 15 at the first intermediary entity 13 whilst second transacting entity 12 will have a second bank account 16 at second intermediary entity 14. Settlement of any given transaction requires instruction given by first transacting entity 11 to its first intermediary entity 13 to pay an agreed amount from the first bank account 15 to the bank account comprising second bank account 16 of second intermediary entity 14 of second transacting entity 12. For these instructions to be carried out metadata in the form of payment metadata 17 must be assembled at the first intermediary entity 13 sufficient and exhaustive to communicate to the second intermediary entity 14 such that the agreed settlement amount is transmitted from bank A to bank B and more particularly to the specific accounts of the respective first transacting entity 11 and second transacting entity 12.

[00036] A similar transaction may be applied in reverse where the second transacting entity sells a good or service to first transacting entity 11. In such an instance the respective intermediaries, once having received the respective payment metadata 17 and exchanged that metadata 17 may elect to simply pay the difference 18 electronically as between the intermediaries to effect the multiple transactions. In some instances, particularly where the transaction is cross-border-for example the first intermediary entity 13 is in a first country whilst the second intermediary entity 14 is in a second country the metadata 17 may include what is known as a Swift code which is a substantially unique identifier for each intermediary entity involved in the transaction. However, for any given transaction, far more data than merely a unique identifier for each intermediary entity involved in a transaction is required in order for the appropriate settlement amounts to ultimately be recorded in the correct accounts and settle the transaction for the agreed amounts.

[00037] Figure 1B is a data and funds flow diagram of data and funds flow according to a prior art settlement system at the granular level. In this instance, with reference to figure 1B pay like components are numbered as for figure 1 a given transaction requiring settlement can be embodied as a bill 90 which will include payment data 91 and may include bank facilitation payment data 92 comprising, in this instance, a biller code and a transaction code. Banks which are party to this bank facilitation payment system permit data entry by entity B (or payer B) 12 into a database of bank B 14 by means of a bank application or web interface 14 B. Bank B may then add additional data to form metadata 17 which is sent to a third-party server 93 which utilises metadata 17 to trigger pay (settlement) of bill 90 from payer B bank 14 to biller A bank 13.

2015903292 14 Aug 2015

[00038] **Generalised Embodiment:**

With reference to Figure 2C there is illustrated a block diagram of the basic infrastructure and components suited for use with embodiments of the present invention. In this instance like components are numbered as for figure 1 except in the 100 series. So, for example, first transacting entity 11 becomes first transacting entity 111 in this embodiment with reference to figure 2C.

In this instance a settlement system 110 according to a generalised embodiment includes at least first transacting entity 111 which enters into a transaction with at least a second transacting entity 112. As previously these entities are associated with a respective first intermediary entity 113 and a second intermediary entity 114 in the form of bank A and bank B. Each of the first transacting entity 111 and a second transacting entity 112 has a respective account 115, 116 at their respective intermediary entities as illustrated in figure 2C

In this instance, in the event that first transacting entity 111 enters into a transaction with second transacting entity 112 then, at the time of entry into the transaction 120, a token 121 is generated. In this instance the token 121 is generated by at least first digital device 122 communicating with a token database 123. The token database 123 generates a token comprising a data file 124 containing all data that will ultimately be required to settle the transaction 120 including any necessary identifying information for the transacting entity is, their accounts and the intermediary entities. Settlement is effected by communication of the token 121 to bank A and then to bank B together with the appropriate flow of funds.

With reference to figure 2A at the granular level a bill 190 from a bill of 111 directed to a payer 112 contains bill data 191 and also token data of a token 121 residing within a code symbol 194 (in this instance a QR code). The token data includes pointer data pointing to data 195 on token database 123. The Dato 195 combined with bank ID data 114 permits the creation by token database 123 of a full payment record 196 which can be utilised to cause settlement of the bill 190 as against payer 112 via, in this instance, their respective banks 114, 113.

With reference to figure 2B the payment data record 196 is utilised has fed into a settlement network such as, for example a network 197 operating under the Ripple protocol thereby permitting substantially real-time settlement across multiple institutions and banks.

2015903292 14 Aug 2015

[00039] **First Embodiment:**

[00040] With reference to Figures 3 there is illustrated in block diagram form a first preferred embodiment of the present invention by way of a non-limiting example of a transaction. In this embodiment like components are numbered as for the previous embodiments except in the 200 series. So, for example, token 121 becomes token 221.

[00041] With reference to figure 3A the transaction system 210 is activated, as for the previous embodiment, when a transaction 220 is entered into between at least first transacting entity 211 and at least a second transacting entity 212 each dealing, for the purposes of this transaction, through respective intermediary entities 213, 214.

[00042] At the time of and as part of entry into the transaction 220 the first transacting entity 211 accesses token database 223 via digital device 222 executing via a web browser interface or via execution of an application running on a portable digital devices such as a mobile telephone or in a further alternative as a point-of-sale terminal in order to arrange for the database 223 to generate a token 221. In this instance the token 221 will include better data 224 including the recipient named, BIC, IBAN, destination country, mobile number, currency, business type, communication, payment amount. In this instance the token 221 including the metadata 224 is stored in the token database 223. In addition the first transacting entity 211 communicates the token 221 to a digital device 230 associated with second transacting entity 212. In this instance the communication is by way of initial transmission of the token 221 to digital device 222 which then on transmits the token via Internet 231 to digital device 230.

[00043] With reference to figure 3B, when ready to settle the transaction 220 the second transacting entity 212 "logs in" to a portal associated with second intermediary entity 214 and communicates the token 221. In this instance have the login can be executed via a web browser associated with digital device 230 which communicates via Internet 231 the token 221 to a digital processing system 232 (including at least a processor and a memory) associated with second intermediary entity 214. Substantially at the same time as part of seeking to settle the transaction 220:

[00044] Notification: token database 223 notifies second intermediary entity 214 to contact the token database 223 from which it receives a further token 221A.

[00045] Verification: token database 223 communicates with the processing system 232 of second intermediary entity 214 to verify that sufficient funds are located in account 216 as indicated in the meta data 224 to settle the transaction

[00046] Committing payer funds: payers bank debits payers account: payers bank sends notice to payer bank gateway: payers bank gateway calls token database 223 to get approved token:

2015903292 14 Aug 2015

[00047] Settlement: gateway of payers bank sends XRP to billers bank gateway: payers bank gateway notifies token database 223 of receipt:

[00048] Clearing: payer's bank Nostro account is debited subject to bank institution rules.

[00049] Embodiments of the invention can be implemented utilising the "Ripple" the framework, protocol and gateway-or more generally any block chain based framework. In a particular form the final settlement process can be enabled through a Ripple frame work thereby to facilitate substantially real-time settlement across multiple institutions and multiple banks.

[00050]

[00051] **Second Embodiment:**

Examples of tokenised messages and their generation and transmission are illustrated in pseudocode below. Reference to "sparro" is a reference to an instance of a token database123.

[00052] The previous, meta-data mode is first. It switches to minimal half way through

--

Bank:HSBC >> createUserCode >> Sparro:Sparro

{"id":"User:ABC Paper","name":"ABC Paper"}

(Creating Sparro User Code - Meta-data given can be used by other banks for compliance and for confirming payee with customers.)

--

Bank:MayBank >> createUserCode >> Sparro:Sparro

{"id":"User:XYZ Printing","name":"XYZ Printing"}

(Creating Sparro User Code - Meta-data given can be used by other banks for compliance and for confirming payee with customers.)

--

Sparro:Sparro >> createUserCode-reply >> Bank:HSBC

{"id":"User:ABC Paper","name":"ABC Paper","code":"65q3gdd"}

--

Sparro:Sparro >> createUserCode-reply >> Bank:MayBank

{"id":"User:XYZ Printing","name":"XYZ Printing","code":"70wqgx6"}

2015903292 14 Aug 2015

--

User:ABC Paper >> createInvoice >> Bank:HSBC

{"amount":{"amount":1000,"currency":"gbp"}}

--

Bank:HSBC >> createInvoiceCode >> Sparro:Sparro

{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd"}

(Creating Invoice Code - An invoice code is created by Sparro and connected to the bank.)

-

Sparro:Sparro >> createInvoiceCode-reply >> Bank:HSBC

{"code":"6tq6wcbad"}

--

Bank:HSBC >> createInvoice-reply >> User:ABC Paper

{"invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

Abc invoice { amount: { amount: 1000, currency: 'gbp' },
payee: '65q3gdd',
code: '6tq6wcbad' }

--

User:ABC Paper >> invoice >> User:XYZ Printing

{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}

-

User:XYZ Printing >> payInvoice >> Bank:MayBank

{"invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300}}

--

Bank:MayBank >> sendMoney >> BankGateway:MayBank

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300}}

--

BankGateway:MayBank >> getInvoice >> Sparro:Sparro

"6tq6wcbad"

(Sending Payment to Invoice - The payment is sent to the bank that created the invoice.)

2015903292 14 Aug 2015

--

Sparro:Sparro >> getInvoice-reply >> BankGateway:MayBank

{"bank":"Bank:HSBC","invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

--

BankGateway:MayBank >> transfer >> BankGateway:HSBC

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":"ripple-1"}

--

BankGateway:HSBC >> incomingTransfer >> Bank:HSBC

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":"ripple-1"}

--

BankGateway:HSBC >> transfer-reply >> BankGateway:MayBank

{"success":true,"owed":{"GBP":300}}

--

Bank:HSBC >> getInvoice >> Sparro:Sparro

"6tq6wcbad"

--

BankGateway:MayBank >> sendMoney-reply >> Bank:MayBank

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":"ripple-1"}

--

Sparro:Sparro >> getInvoice-reply >> Bank:HSBC

{"bank":"Bank:HSBC","invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

2015903292 14 Aug 2015

--

Bank:MayBank >> payInvoice-reply >> User:XYZ Printing

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":"ripple-1"}

XYZ part-paid invoice {
"payer": "70wqgx6",
"invoice": "6tq6wcbad",
"amount": {
"currency": "GBP",
"amount": 300
},
"id": "ripple-1"
}

--

Bank:HSBC >> incomingTransfer >> User:ABC Paper

{"invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"},"transfer":{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":"ripple-1"}}

-

User:XYZ Printing >> payInvoice >> Bank:MayBank

{"invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700}}

--

Bank:MayBank >> sendMoney >> BankGateway:MayBank

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700}}

--

BankGateway:MayBank >> getInvoice >> Sparro:Sparro

"6tq6wcbad"

14 Aug 2015 2015903292

(Sending Payment to Invoice - The payment is sent to the bank that created the invoice.)

--

Sparro:Sparro >> getInvoice-reply >> BankGateway:MayBank

{"bank":"Bank:HSBC","invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

--

BankGateway:MayBank >> transfer >> BankGateway:HSBC

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700},"id":"ripple-2"}

--

BankGateway:HSBC >> incomingTransfer >> Bank:HSBC

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700},"id":"ripple-2"}

--

BankGateway:HSBC >> transfer-reply >> BankGateway:MayBank

{"success":true,"owed":{"GBP":1000}}

--

Bank:HSBC >> getInvoice >> Sparro:Sparro

"6tq6wcbad"

-

BankGateway:MayBank >> sendMoney-reply >> Bank:MayBank

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700},"id":"ripple-2"}

2015903292 14 Aug 2015

--

Sparro:Sparro >> getInvoice-reply >> Bank:HSBC

{"bank":"Bank:HSBC","invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

--

Bank:MayBank >> payInvoice-reply >> User:XYZ Printing

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700},"id":"ripple-2"}

XYZ finished paying invoice {
 "payer": "70wqgx6",
 "invoice": "6tq6wcbad",
 "amount": {
  "currency": "GBP",
  "amount": 700
 },
 "id": "ripple-2"
}

--- SWITCHING TO MODE: minimal ---

--

Bank:HSBC >> incomingTransfer >> User:ABC Paper

{"invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"},"transfer":{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700},"id":"ripple-2"}}

--Bank:HSBC >> createUserCode >> Sparro:Sparro

2015903292 14 Aug 2015

undefined
(Creating Sparro User Code - No meta-data is required.)

--
Bank:MayBank >> createUserCode >> Sparro:Sparro
undefined
(Creating Sparro User Code - No meta-data is required.)

--
Sparro:Sparro >> createUserCode-reply >> Bank:HSBC
{"code":"dnt7gec"}

--
Sparro:Sparro >> createUserCode-reply >> Bank:MayBank
{"code":"6wwpwuc"}

--
User:ABC Paper >> createInvoice >> Bank:HSBC
{"amount":{"amount":2000,"currency":"gbp"}}

--
Bank:HSBC >> createInvoiceCode >> Sparro:Sparro
null
(Creating Invoice Code - An invoice code is created by Sparro and connected to the bank. No invoice details are required.)

--
Sparro:Sparro >> createInvoiceCode-reply >> Bank:HSBC
{"code":"erwkax1md"}

--Bank:HSBC >> createInvoice-reply >> User:ABC Paper

2015903292 14 Aug 2015

{"invoice":{"amount":{"amount":2000,"currency":"gbp"},"code":"erwkax1md","payee":"User:
ABC Paper","transfers":[]}}

Abc invoice { amount: { amount: 2000, currency: 'gbp' },
code: 'erwkax1md',
payee: 'User:ABC Paper',
transfers: [] }

--

User:ABC Paper >> invoice >> User:XYZ Printing

{"amount":{"amount":2000,"currency":"gbp"},"code":"erwkax1md","payee":"User:ABC
Paper","transfers":[]}

--

User:XYZ Printing >> payInvoice >> Bank:MayBank

{"invoice":"erwkax1md","amount":{"currency":"GBP","amount":600}}

--

Bank:MayBank >> sendMoney >> BankGateway:MayBank

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600}}

--

BankGateway:MayBank >> getInvoice >> Sparro:Sparro

"erwkax1md"

(Sending Payment to Invoice - The payment is sent to the bank that created the invoice.)

--

Sparro:Sparro >> getInvoice-reply >> BankGateway:MayBank

{"bank":"Bank:HSBC"}

--

BankGateway:MayBank >> transfer >> BankGateway:HSBC

2015903292 14 Aug 2015

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}

--

BankGateway:HSBC >> incomingTransfer >> Bank:HSBC

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}

--

BankGateway:HSBC >> transfer-reply >> BankGateway:MayBank

{"success":true,"owed":{"GBP":600}}

--

Bank:HSBC >> incomingTransfer >> User:ABC Paper

{"invoice":{"amount":{"amount":2000,"currency":"gbp"},"code":"erwkax1md","payee":"User:ABC Paper","transfers":[{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}]},"transfer":{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}}

--

BankGateway:MayBank >> sendMoney-reply >> Bank:MayBank

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}

--

Bank:MayBank >> payInvoice-reply >> User:XYZ Printing

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}

2015903292 14 Aug 2015

XYZ part-paid invoice {
"payer": "6wwpwuc",
"invoice": "erwkax1md",
"amount": {
"currency": "GBP",
"amount": 600
},
"id": "ripple-3"
}
--
User:XYZ Printing >> payInvoice >> Bank:MayBank
{"invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400}}

--
Bank:MayBank >> sendMoney >> BankGateway:MayBank

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400}}

--
BankGateway:MayBank >> getInvoice >> Sparro:Sparro
"erwkax1md"
(Sending Payment to Invoice - The payment is sent to the bank that created the invoice.)

--
Sparro:Sparro >> getInvoice-reply >> BankGateway:MayBank
{"bank":"Bank:HSBC"}

-
BankGateway:MayBank >> transfer >> BankGateway:HSBC

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}

2015903292 14 Aug 2015

--

BankGateway:HSBC >> incomingTransfer >> Bank:HSBC

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}

BankGateway:HSBC >> transfer-reply >> BankGateway:MayBank

{"success":true,"owed":{"GBP":2000}}

--

Bank:HSBC >> incomingTransfer >> User:ABC Paper

{"invoice":{"amount":{"amount":2000,"currency":"gbp"},"code":"erwkax1md","payee":"User:ABC Paper","transfers":[{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"},{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}]},"transfer":{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}}

--

BankGateway:MayBank >> sendMoney-reply >> Bank:MayBank

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}

--

Bank:MayBank >> payInvoice-reply >> User:XYZ Printing

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}

2015903292 14 Aug 2015

```
XYZ finished paying invoice {
 "payer": "6wwpwuc",
 "invoice": "erwkax1md",
 "amount": {
  "currency": "GBP",
  "amount": 1400
 },
 "id": "ripple-4"
}
```

features of this embodiment include the enablement of a private, invitation only, network for banking institutions which, in a particular form, can facilitate cross-border payments thereby to enable substantially real-time payments at reduced processing cost.

With reference to figure 4 there is shown a block diagram of salient characteristics of a messaging system 10 of the prior art as compared with the salient messaging characteristics of the system 210 enabled by the code listed above and more broadly described with reference to the earlier embodiments.

figure 5 illustrates the options for data content to be included in tokens in accordance with embodiments of the invention as described above.

Figure 6 provides a comparison of characteristics of embodiments of the present invention as compared with the prior art Swift-based messaging system at a commercial layer 470, a security layer 471 and a technical layer 472.

[00053] The above describes only some embodiments of the present invention and modifications, obvious to those skilled in the art, can be made thereto without departing from the scope of the present invention.

2015903292 14 Aug 2015

CLAIMS

1. A system for settling a transaction electronically; said system comprising:
at least a first transacting entity;
at least a second transacting entity;

at least a first intermediary entity;
at least a second intermediary entity;
in the case where the first transacting entity enters into a transaction with the second transacting entity generating a tokenised message at the time of the transaction containing data needed to settle the transaction;
initiating settlement of the transaction by transmission of the tokenised message to the at least first transacting entity.

2. The system of claim 1 wherein the tokenised message is generated with reference to a token database located at a remote location.

3. The system of claim 2 wherein the tokenised message includes at least a first data element, a second data element and a third data element.

4. The system of claim 3 wherein the first data element comprises identification data for a payor, the second data element comprises identification data for a payee (biller) and the third data element comprises identification currency, denomination and value data.

5. The system of claim 1 or claim 2 wherein a further tokenised message is generated by either an intermediary entity or the token database.

6. The system of any previous claim where in a tokenised message is generated by a bi-directional communication process.

7. The system of claim 6 wherein the bi-directional communication process is between the token database and an intermediary entity.

8. The system of any previous claim wherein a step in producing a tokenised message involves de-identifying data.

9. The system of any previous claim wherein a step in producing a tokenised message involves adding a data element to the message.

10. The system of any previous claim wherein a step in producing a tokenised message involves removing a data element from the message.

11. The system of any previous claim wherein a step in producing a tokenised message involves applying an algorithm to the data elements in the message.

2015903292 14 Aug 2015

12. The system of any previous claim wherein the token database sequences the tokenised messages.

13. The system of any previous claim wherein the token database sequences the tokenised messages and transmits the tokenised messages as payment data records to a block chain settlement system.

14. The system of claim 13 wherein the block chain settlement system employs the Ripple protocol.

15. A tokenised message construction system; said system comprising:
a server in communication with a database and which facilitates communications between a plurality of parties to a transaction;
each party having a digitised device with which to communicate with other ones of the parties and with the server;
each party capable of generating a tokenised message via a bidirectional communication with the server.

16. The system of claim 15 wherein the tokenised message is generated with reference to a token database located at a remote location.

17. The system of claim 16 wherein the tokenised message includes at least a first data element, a second data element and a third data element.

18. The system of claim 17 wherein the first data element comprises identification data for a payor, the second data element comprises identification data for a payee (biller) and the third data element comprises identification currency, denomination and value data.

19. The system of claim 15 or claim 16 wherein a further tokenised message is generated by either an intermediary entity or the token database.

20. The system of any one of claims 15 to 19 wherein a tokenised message is generated by a bi-directional communication process.

21. The system of claim 20 wherein the bi-directional communication process is between the token database and an intermediary entity.

22. The system of any one of claims 15 to 21 wherein a step in producing a tokenised message involves de-identifying data.

23. The system of any one of claims 15 to 22 wherein a step in producing a tokenised message involves adding a data element to the message.

24. The system of any one of claims 15 to 23 wherein a step in producing a tokenised message involves removing a data element from the message.

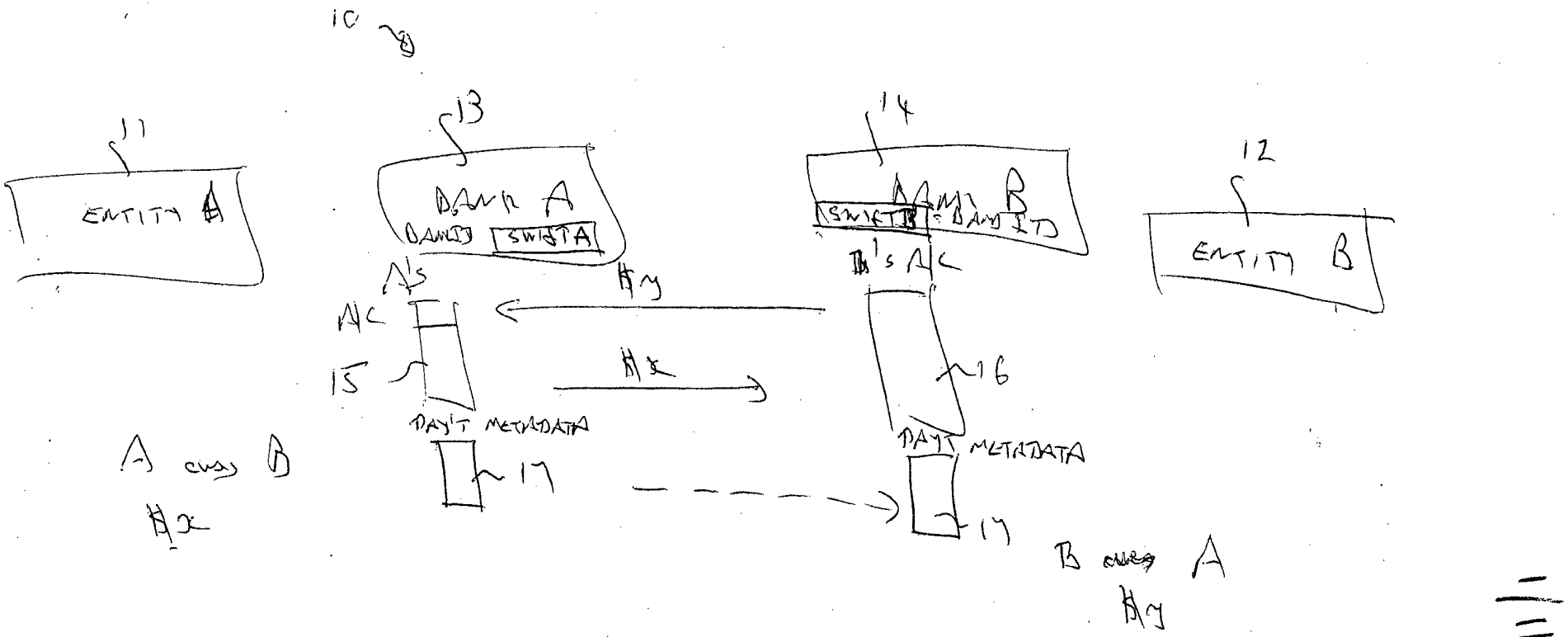
2015903292 14 Aug 2015

25. The system of any one of claims 15 to 24 wherein a step in producing a tokenised message involves applying an algorithm to the data elements in the message.

26. The system of any one of claims 15 to 25 wherein the token database sequences the tokenised messages.

27. The system of any one of claims 15 to 26 wherein the token database sequences the tokenised messages and transmits the tokenised messages as payment data records to a block chain settlement system.

28. The system of claim 27 wherein the block chain settlement system employs the Ripple protocol.



ALT :- any #Δ(x-y)

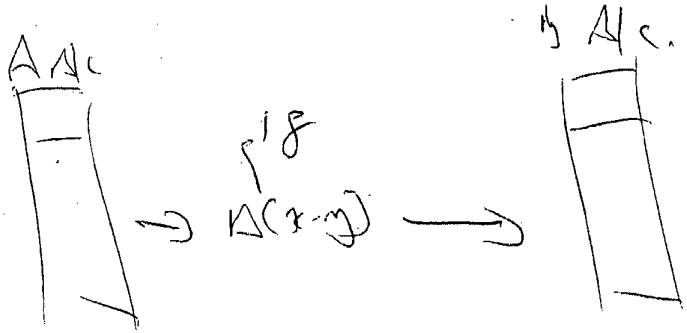


Fig 1A

[Prior Art]

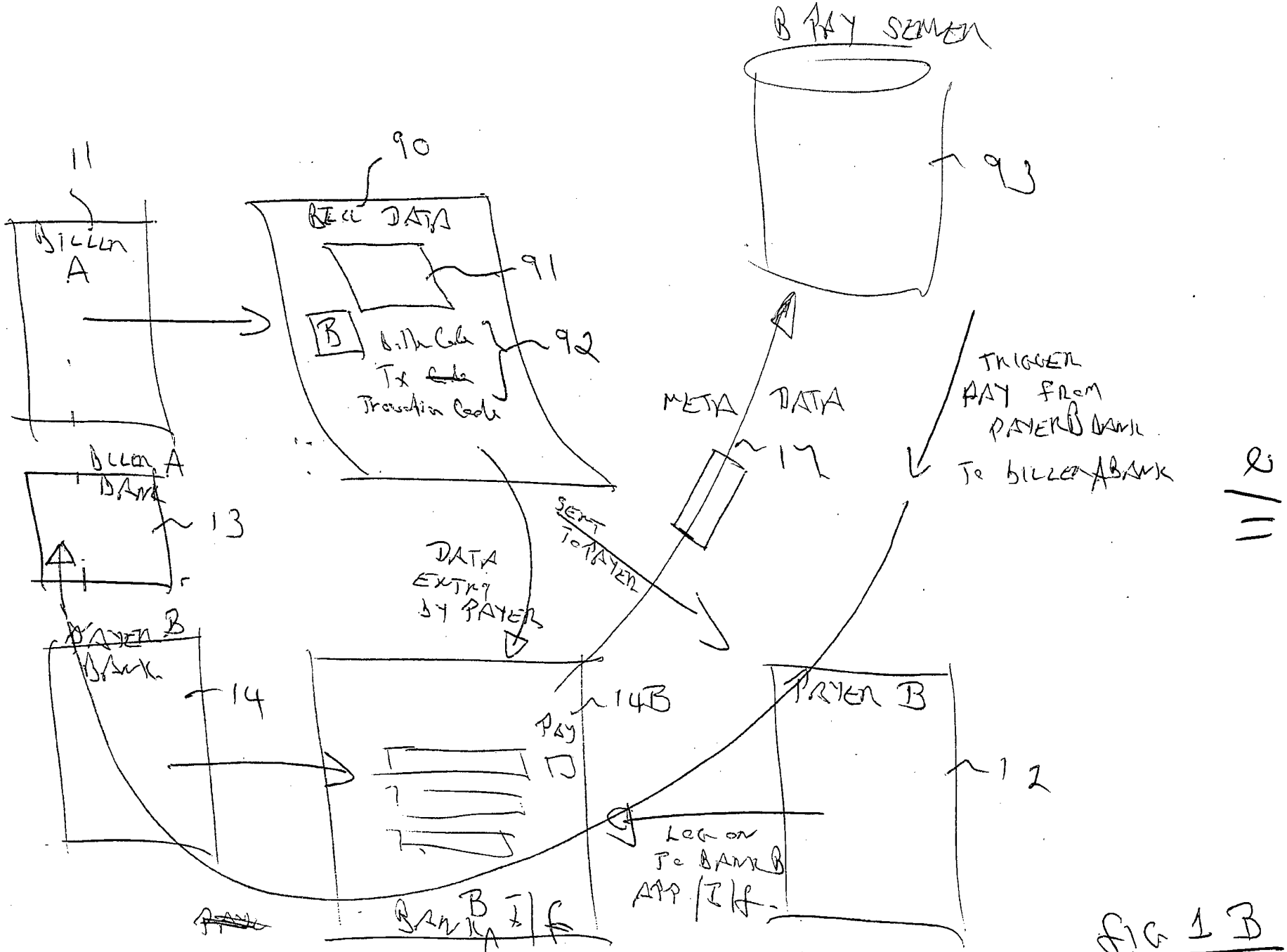
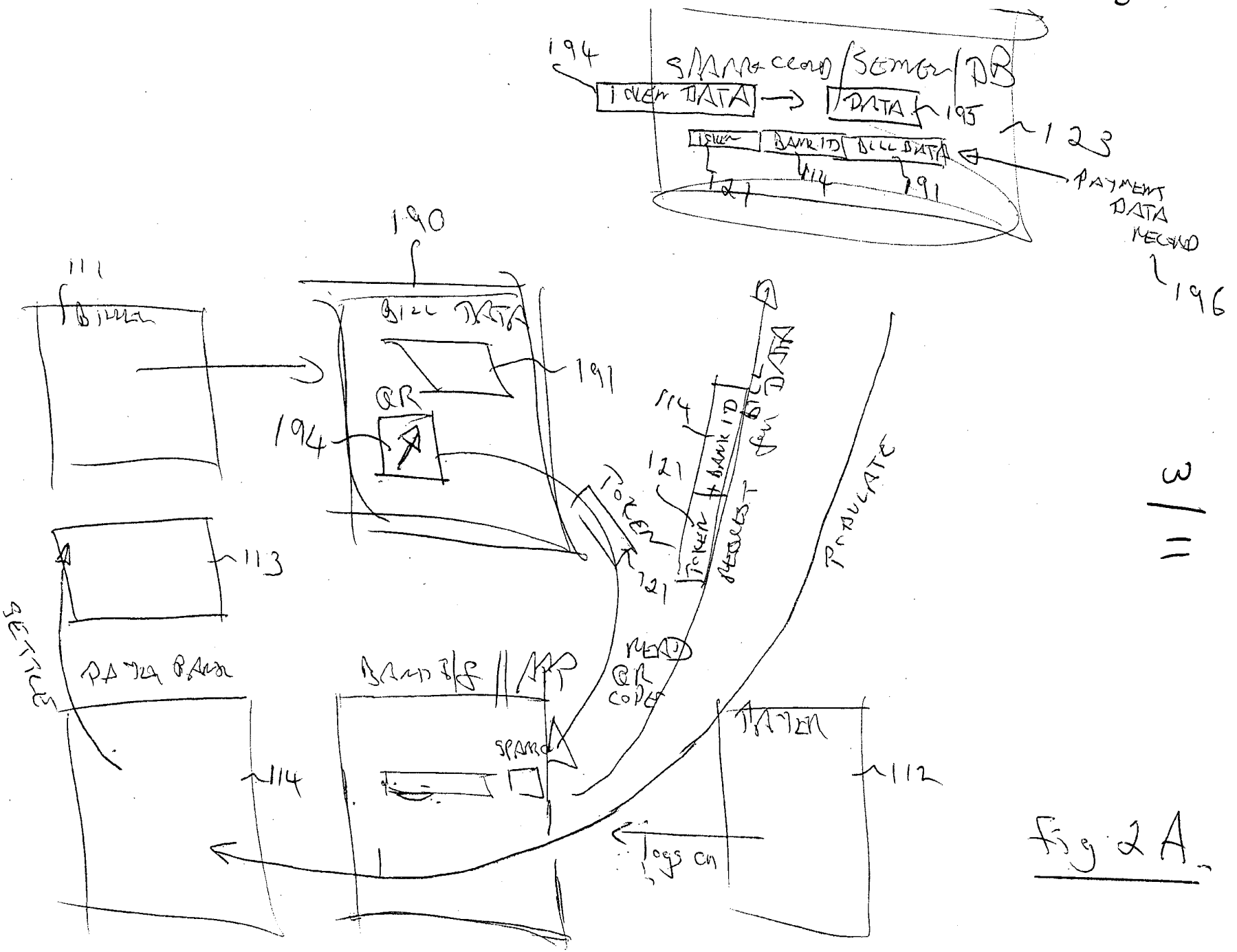

B PAY SERVER
93
11
BILLER A
90
REC DATA
91
B
92
Tx
Transaction Code
META DATA
17
TRIGGER
PAY FROM
PAYER B BANK
To BILLER A BANK
BILLER A
BANK
13
SENT
TO PAYER
DATA
ENTRY
BY PAYER
PAYER B
BANK
14
14B
PAY
ID
PAYER B
12
LOG on
To BANK B
APP I/F
BANK B I/F

Fig 1B


194
ISSUER DATA
DATA
195
123
ISSUER
BANK ID
BILL DATA
114
191
121
PAYMENT DATA RECORD
196
190
111
BILLER
BILL DATA
191
QR
194
114
121
BANK ID
BILL DATA
TOKEN
REQUEST
TOKEN
113
PRE-POPULATE
SETTLE
DATA BASE
BANK APP
RECEIVE QR CODE
SPARE
114
PAYER
112
LOGS ON

3/11

Fig 2A.

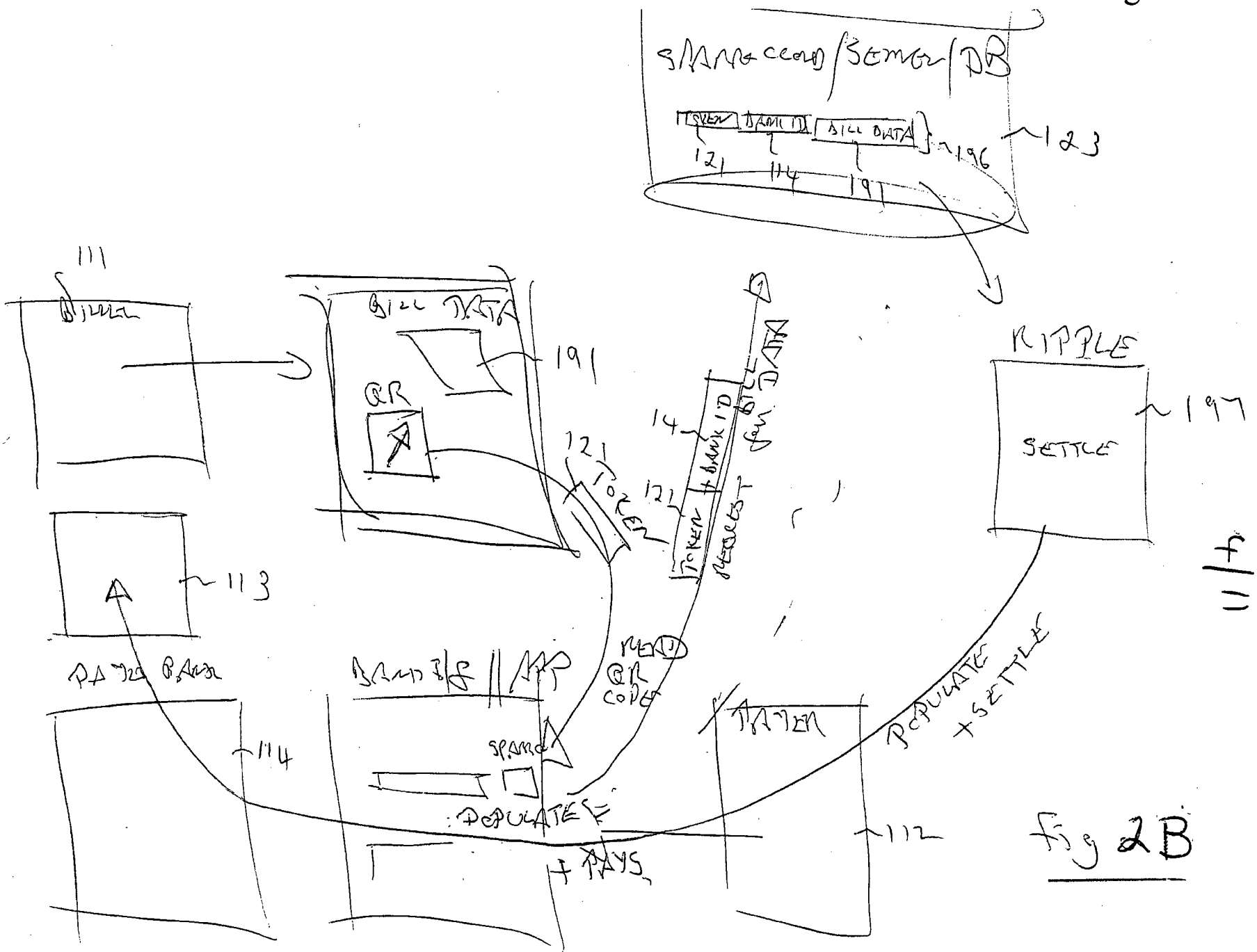

SMARTPHONE/SERVER/DB
SERVER
BANK ID
BILL DATA
121
114
191
196
123
111
BILLER
BILL DATA
191
QR
121
TOKEN
14
BANK ID
BILL DATA
121
TOKEN
REQUEST
RIPPLE
SETTLE
197
113
PAYER BANK
BANK B/E
APP
114
QR CODE
SPARE
DUPLICATE
+ PAYS
PAYEE
112
REPLICATE
+SETTLE

Fig 2B

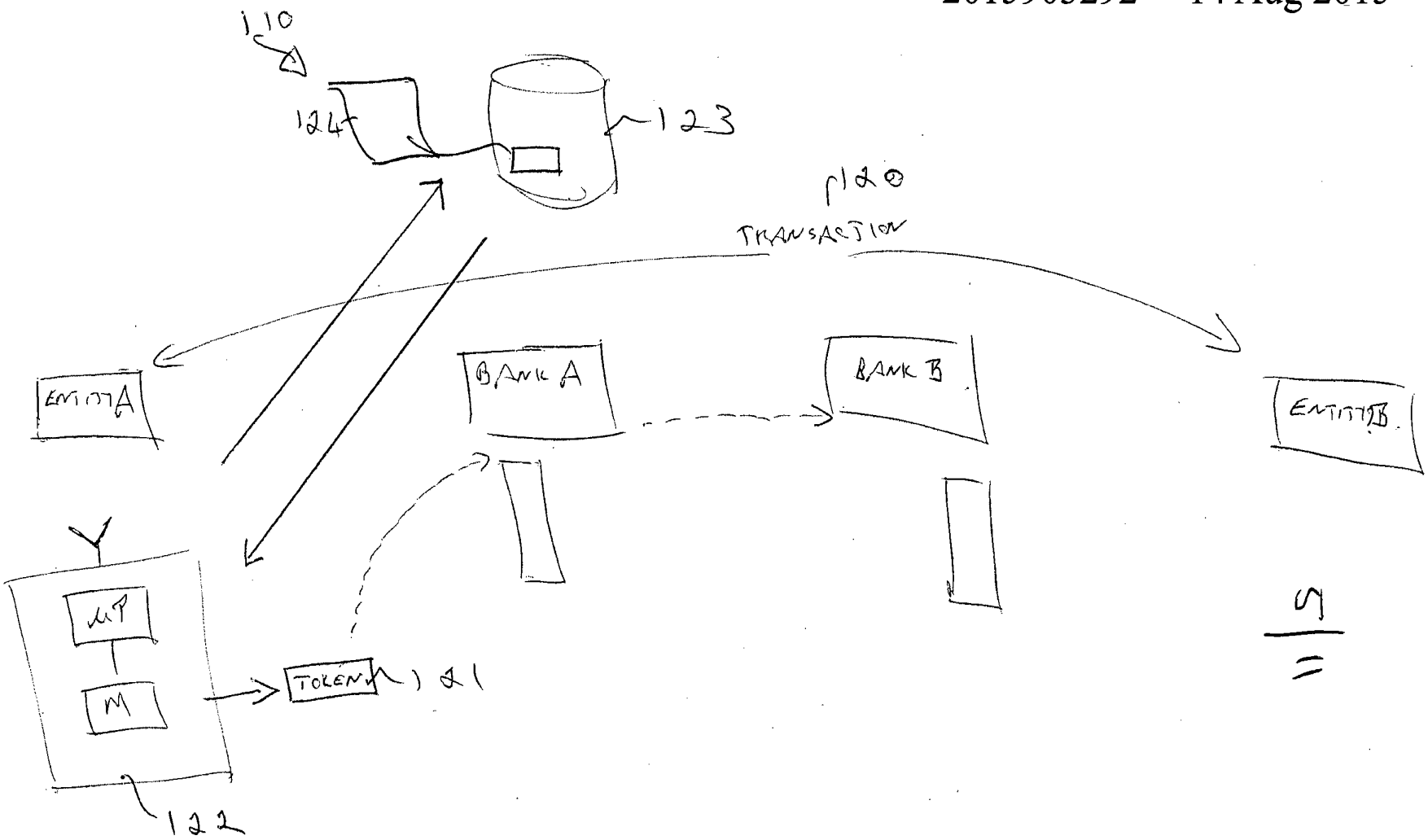


Fig 2 C.

JPMC Ex. 1002
Page 395

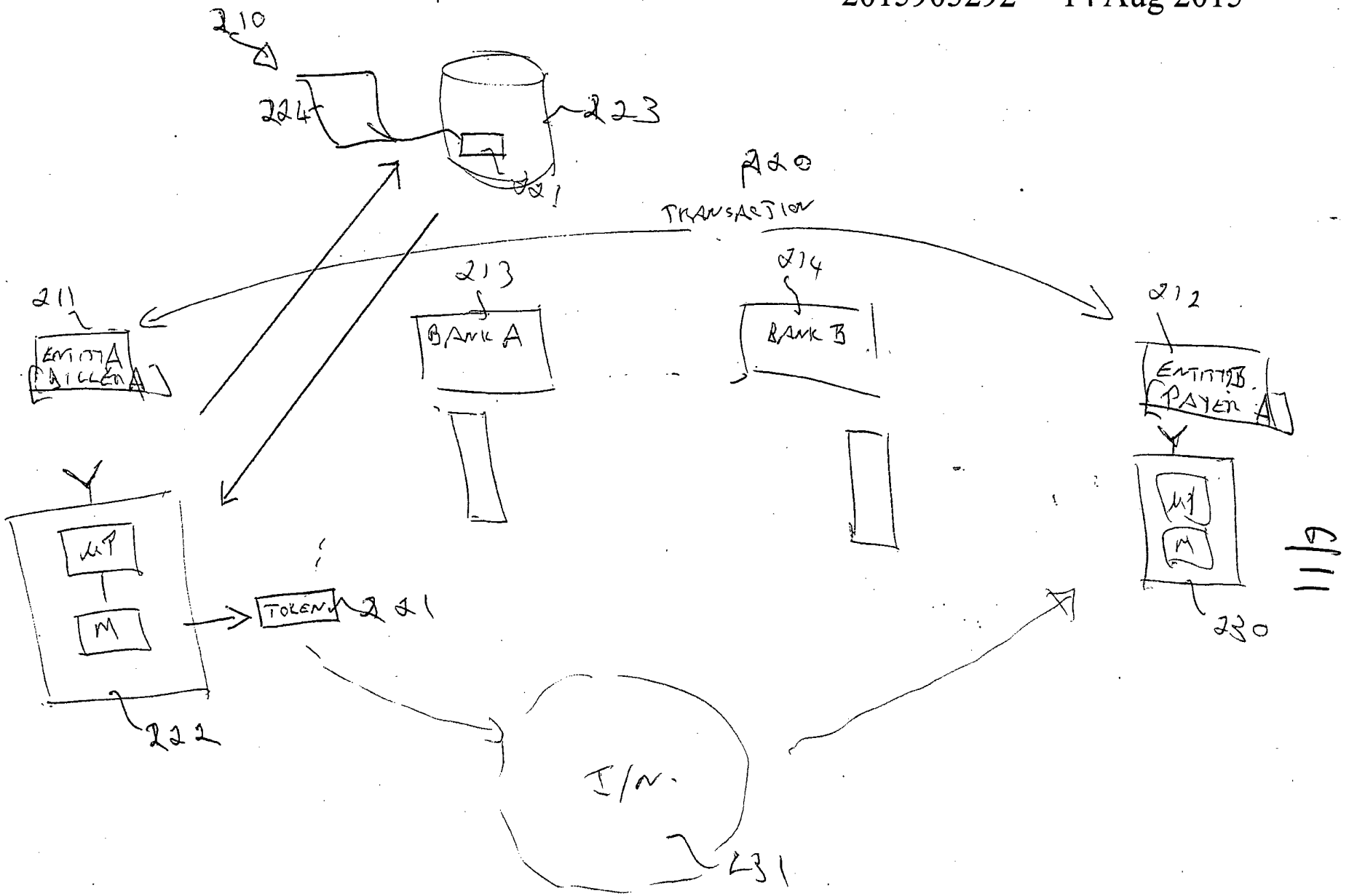

210
224
223
221
220
TRANSACTION
211
ENTITY A
CALLER A
213
BANK A
214
BANK B
212
ENTITY B
PAYER A
MP
M
TOKEN
241
222
I/N.
231
230

Fig 3A

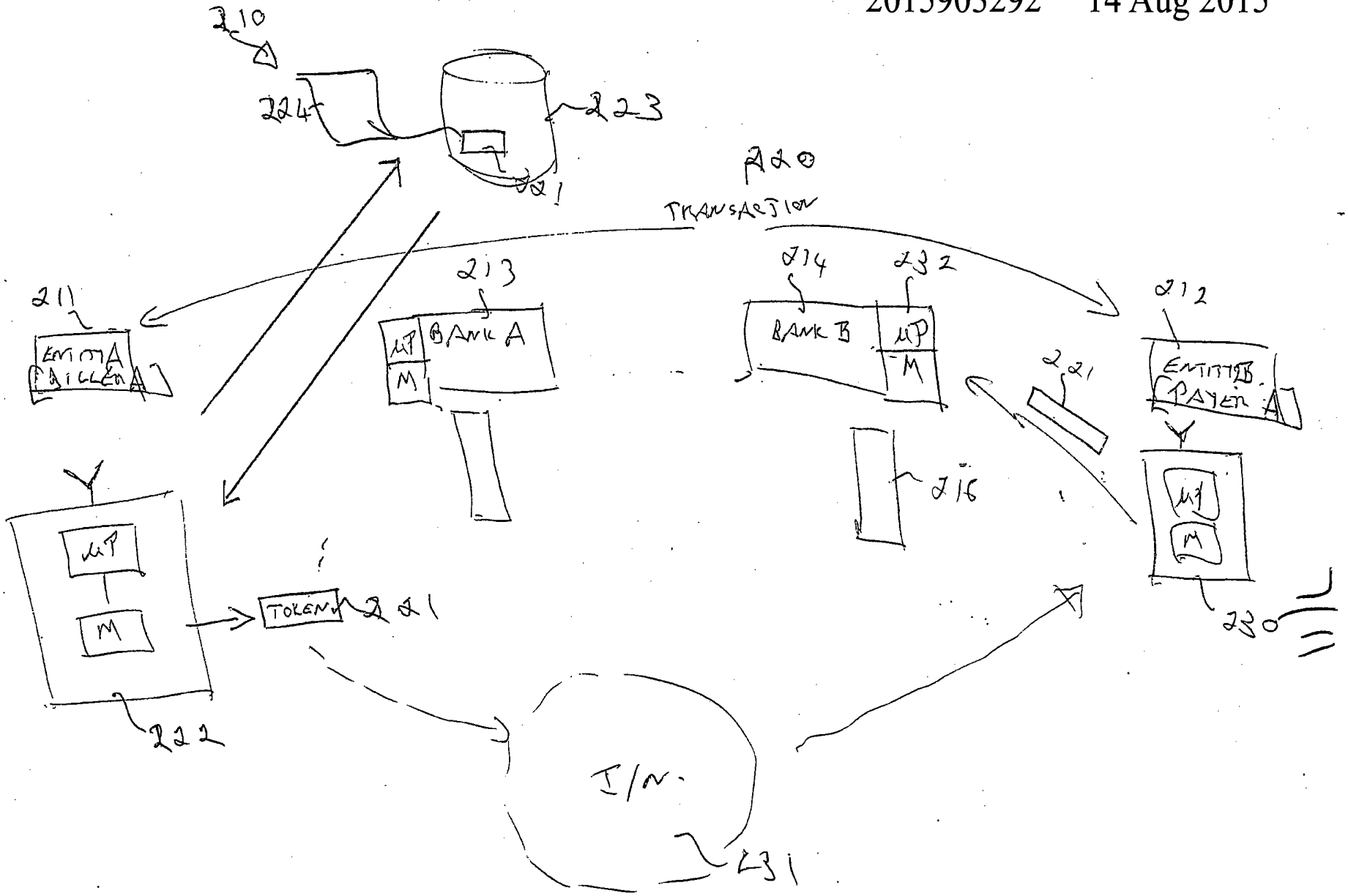

TCR
210
224
223
221
220
TRANSACTION
211
ENTITY A
PAYER A
213
BANK A
μP
M
214
232
BANK B
μP
M
216
221
212
ENTITY B
PAYER A
μP
M
222
TOKEN
241
I/N.
231
230

Fig 3B

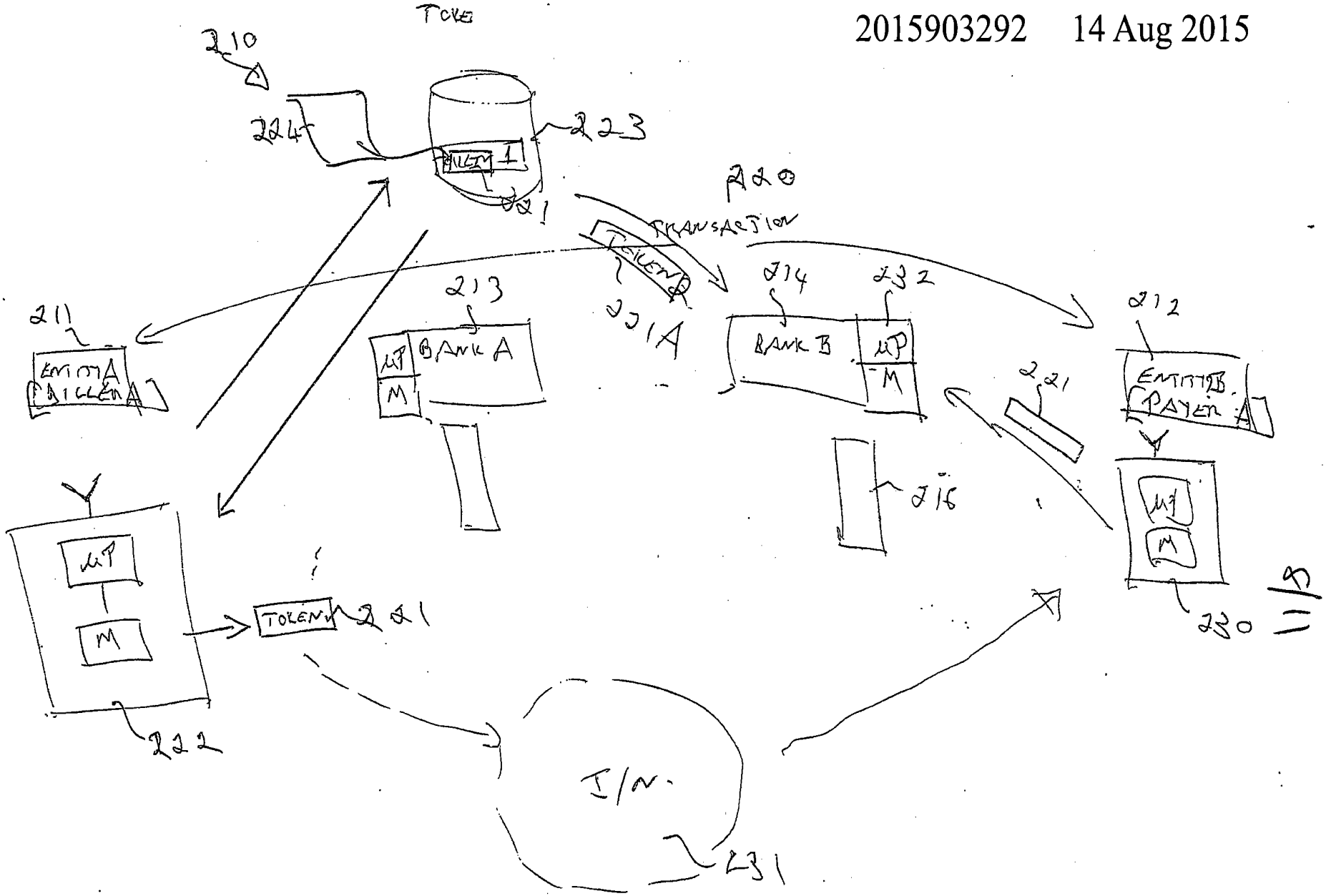
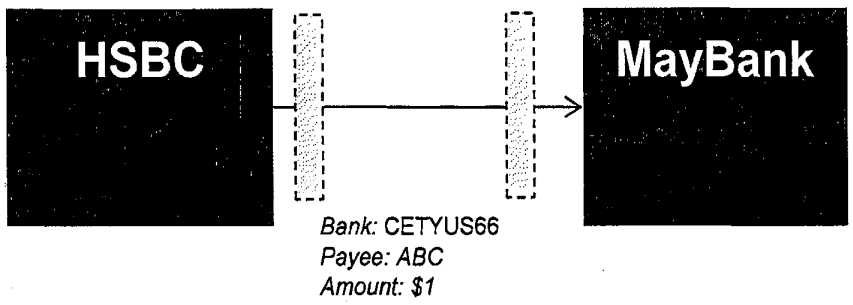

TOKEN
210
224
223
TOKEN 1
221
220
TRANSACTION
TOKEN
231A
211
ENTITY A
CALLER A
213
BANK A
214
BANK B
232
212
ENTITY B
PAYEE A
221
216
TOKEN
241
222
220
I/N.
231

Fig 3C

JPMC Ex. 1002
Page 399

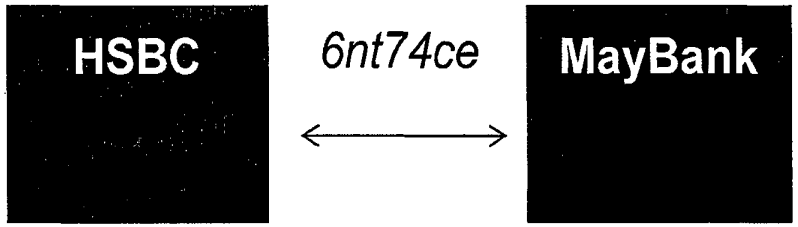
Our token system gives power back to Banks run their own shop; with their own, decentralized security management

Existing (SWIFT) system



(a) Depends on SWIFT infrastructure

Proposed system



(a) Bank-originating (cuts costs)

(b) Optional add-on: Data-enriched for PaaS for customers

14 Aug 2015 20159032921.s

JPMC Ex. 1002
Page 400

We can curate our messaging system to accommodate Bank's risk appetite in relation to user data

Base case	Option A: XX	Option B: Data rich
Fully anonymized data	**Text** • Text - Text	**User ID shared with Sparro**
Bank-powered • Tokenization within bank • User ID generation in banks		**Bank-powered** • Tokenization within bank • User ID generation in banks
Benefit • Processing cost • Improved confidentiality of transaction data		**Benefit** • Processing costs • Enriched Payments as a Service to Bank customers

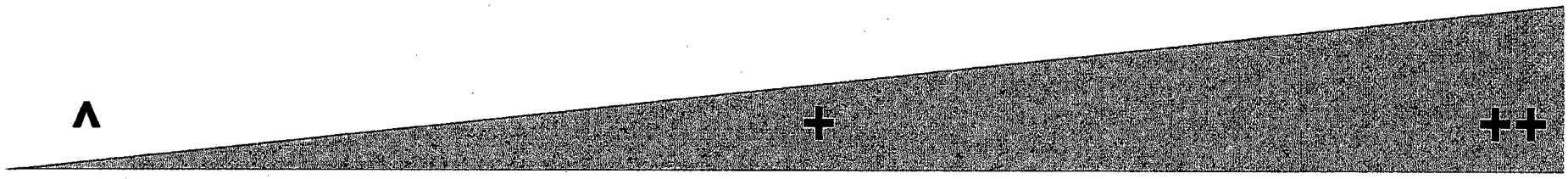


Fig 5

14 Aug 2015 2015903292

SUMMARY: Benefits to Banks vis-a-vis SWIFT and Ripple

Issue	SWIFT	Ripple	Proposed
Commercial	Bypass SWIFT	No competition, given infrastructure focus	1. Banks turn cost centre re SWIFT processing into profit pool 2. *Optional add-on:* new revenue from e.g. PaaS
Security	SWIFT-based	Block chain	1. Bank's private system
Technical	Committed infrastructure spend is slow & expensive	Private gateway establishment	Sparro (anonymized) messaging

fig 6.

14 Aug 2015 20159032 92

WIPO
WORLD
INTELLECTUAL PROPERTY
ORGANIZATION

DOCUMENT MADE AVAILABLE UNDER THE PATENT COOPERATION TREATY (PCT)

International application number:		**PCT/AU2016/000279**
International filing date:		**12 August 2016 (12.08.2016)**
Document type:		**Certified copy of priority document**
Document details:	Country/Office:	**AU**
	Number:	**2015903292**
	Filing date:	**14 August 2015 (14.08.2015)**
Date of receipt at the International Bureau:		**27 September 2016 (27.09.2016)**

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a),(b) or (b-*bis*)

34, chemin des Colombettes
1211 Geneva 20, Switzerland
www.wipo.int

Australian Government

PCT/AU2016/000279

Patent Office
Canberra

I, VIVIENNE IGLESIAS, DELEGATE OF THE COMMISSIONER, hereby certify that annexed is a true copy of the Provisional specification in connection with Application No. 2016901924 for a patent by SPARRO (AUSTRALIA) PTY LTD as filed on 20 May 2016.

WITNESS my hand this
THIRTEENTH day of September 2016

VIVIENNE IGLESIAS
DELEGATE OF THE COMMISSIONER

COMMONWEALTH OF AUSTRALIA
AUSTRALIA
PATENT OFFICE

2016901924 20 May 2016

Payment Messaging System

TECHNICAL FIELD

[0001] The present invention relates to settlement systems and, more particularly although not exclusively, to a payment messaging system particularly, although not exclusively, suited to electronic transactions.

BACKGROUND

[0002] "Settlement" in the sense of settling amounts owing as between two parties, whether in a Fiat currency or in the newer forms of electronic currency (such as "Bitcoin") is a known concept which is central to the workings of most financial systems. In the case of electronic currency which requires settlement by exchange of data between institutions the current system is quite cumbersome and leads to many costs due in part to the necessity for often repeated data entry of significant amounts of data into systems run by the parties to any given transaction requiring settlement and also to the intermediaries that it almost every instance (barring a non-electronic cash transaction) form part of a chain of intermediaries that become involved in ultimately effecting settlement of any given transaction.

[0003] In particular implementations of settlement systems across the internet, a blockchain structure may be utilised where a blockchain is a distributed database that maintains a continuously growing list of data records that may be hardened against tampering and revision. The most widely known application of a blockchain is the public ledger of transactions for cryptocurrencies, such as Bitcoin referenced above.

[0004] Many settlement systems are characterised by effectively one-way transmission of data in any given data exchange transaction (for example systems based on Swift messaging). If it is subsequently discovered that there are deficiencies in the data thus transmitted there can then ensue time consuming checking and querying operations before settlement can be effected.

[0005] It is an object of the present invention to address or at least ameliorate some of the above disadvantages.

2016901924 20 May 2016

Notes

[0006] The term "comprising" (and grammatical variations thereof) is used in this specification in the inclusive sense of "having" or "including", and not in the exclusive sense of "consisting only of".

[0007] The above discussion of the prior art in the Background of the invention, is not an admission that any information discussed therein is citable prior art or part of the common general knowledge of persons skilled in the art in any country.

SUMMARY OF INVENTION

Definitions:

[0008] **token:** in this specification a "token" is a data record containing data required to settle a transaction for which the token has been generated; and wherein the data is rendered, formatted or passed through an algorithm in a predetermined manner. The process of rendering, formatting or passing through an algorithm in a predetermined manner is termed "tokenisation". The tokenisation process may involve operations such as encryption and de-identification of data.

[0009] **Transaction:** in this specification "transaction" refers to a trade between two parties, for example at least a first transacting entity and a second transacting entity and wherein the trade is expressed in a financial form (for example in a Fiat currency or an electronic currency-to be distinguished, for example, from a barter transaction) which will ultimately require exchange of currency to settle the transaction. In some instances the currency will be the same on both sides of the transaction. In other cases a conversion from one currency to another may be required.

[00010] **Personally Identifiable Information (PII):** in this specification refers to information that a regulator or privacy policy will not allow to be disclosed to a third party.

[00011] Accordingly, in one broad form of the invention, there is provided a system for settling a transaction electronically; said system comprising:

at least a first transacting entity;

at least a second transacting entity;

at least a first intermediary entity;

at least a second intermediary entity;

2016901924 20 May 2016

in the case where the first transacting entity enters into a transaction with the second transacting entity generating a tokenised message at the time of the transaction containing data needed to settle the transaction;
initiating settlement of the transaction by transmission of the tokenised message to the at least first transacting entity.

[00012] In a further broad form of the invention there is provided a tokenised message construction system; said system comprising:
a server in communication with a database and which facilitates communications between a plurality of parties to a transaction;
each party having a digitised device with which to communicate with other ones of the parties and with the server;
each party capable of generating a tokenised message via a bidirectional communication with the server.

[00013] Accordingly, in yet a further broad form of the invention there is provided tokenised message construction system; said system comprising:
a server in communication with a database and which facilitates communications between a plurality of parties to a transaction;
each party having a digitised device with which to communicate with other ones the parties and with the server;
each party capable of generating a tokenised message via a bidirectional communication with the server.

[00014] Preferably the tokenised message is generated with reference to a token database located at a remote location.

[00015] Preferably the tokenised message includes at least a first data element, a second data element and a third data element.

[00016] Preferably the first data element comprises identification data for a payor, the second data element comprises identification data for a payee (biller) and the third data element comprises identification currency, denomination and value data.

2016901924 20 May 2016

[00017] Preferably a further tokenised message is generated by either an intermediary entity or the token database.

[00018] Preferably a tokenised message is generated by a bi-directional communication process.

[00019] Preferably the bi-directional communication process is between the token database and an intermediary entity.

[00020] Preferably a step in producing a tokenised message involves de-identifying data.

[00021] Preferably a step in producing a tokenised message involves adding a data element to the message.

[00022] Preferably a step in producing a tokenised message involves removing a data element from the message.

[00023] Preferably a step in producing a tokenised message involves applying an algorithm to the data elements in the message.

[00024] Preferably the token database sequences the tokenised messages.

[00025] Preferably the token database sequences the tokenised messages and transmits the tokenised messages as payment data records to a blockchain settlement system.

[00026] Preferably the blockchain settlement system employs the Ripple protocol.

[00027] Preferably the tokenised message includes at least a first data element, a second data element and a third data element.

[00028] Preferably the first data element comprises identification data for a payor, the second data element comprises identification data for a payee (biller) and the third data element comprises identification currency, denomination and value data.

[00029] Preferably a further tokenised message is generated by either an intermediary entity or the token database.

[00030] Preferably a tokenised message is generated by a bi-directional communication process.

2016901924 20 May 2016

[00031] Preferably the bi-directional communication process is between the token database and an intermediary entity.

[00032] Preferably a step in producing a tokenised message involves de-identifying data.

[00033] Preferably a step in producing a tokenised message involves adding a data element to the message.

[00034] Preferably a step in producing a tokenised message involves removing a data element from the message.

[00035] Preferably a step in producing a tokenised message involves applying an algorithm to the data elements in the message.

[00036] Preferably the token database sequences the tokenised messages.

[00037] Preferably the token database sequences the tokenised messages and transmits the tokenised messages as payment data records to a blockchain settlement system.

[00038] Preferably the blockchain settlement system employs the Ripple protocol.

[00039] Preferably a second message is transmitted between the intermediaries.

[00040] Preferably the second message is tokenised.

[00041] Preferably the second message contains conventional data.

[00042] Preferably the second message is transmitted by means of a blockchain system.

[00043] Preferably the second message includes information equivalent to that transmitted by the SWIFT system.

[00044] Preferably the tokenised message includes additional information beyond that transmitted by the SWIFT system.

[00045] The system of claim 35 wherein the tokenised message includes information which verifies the security status of at least one party to the transaction.

2016901924 20 May 2016

[00046] Preferably the second tokenised message includes information which verifies the security status of both parties to the transaction.

[00047] Preferably the token is conveyed by way of a medium utilizing the SWIFT messaging system or other compatible messaging system.

[00048] Preferably the medium is implemented by way of a VPN.

[00049] Preferably deidentified data associated with the transaction to which the token pertains is transmitted over a separate communication medium.

[00050] Preferably the separate communication medium utilizes a blockchain structure.

[00051] Preferably the deidentified data is located within a record structure which is replicated throughout the blockchain structure.

[00052] Preferably in use a sellers bank as part of entering into the transaction with buyers bank will establish a SWIFT transaction.

[00053] Preferably in parallel the sellers bank will perform associated operations needed to complete the transaction such as verification of the buyers ID and related characteristics.

[00054] Preferably data related to the associated operations is then placed in a record structure and that record is placed into the blockchain structure.

[00055] Preferably the associated data includes deidentifed data.

[00056] Preferably the data is available to the buyers bank by way of the buyers bank logging into the blockchain structure and receiving the deidentified data which is associated with the transaction which is represented by the token thereby allowing assembly by the buyers bank of all necessary data to execute the transaction on behalf of the buyer and seller.

[00057] Preferably incorporating secure channels thereby permitting only selected entities to communicate the data to execute the transaction on behalf of the buyer and seller.

BRIEF DESCRIPTION OF DRAWINGS

[00058] Embodiments of the present invention will now be described with reference to the accompanying drawings wherein:

2016901924 20 May 2016

[00059] Figure 1A is a block diagram of the entities and intermediaries involved in a prior art electronic settlement system;

[00060] Figure 1B is a data and funds flow according to a prior art settlement system;

[00061] Figure 2A is a data and funds flow diagram according to an indicative embodiment of the present invention;

[00062] Figure *2C* is a block diagram of the basic infrastructure and components suited for use with embodiments of the present invention and

[00063] Figure 3 A, B, C comprise block diagrams of the steps in a settlement transaction in accordance with a first preferred embodiment of the present invention

[00064] Figure 4 is a block diagram of salient characteristics of a messaging system 10 of the prior art as compared with the salient messaging characteristics of the system 210 enabled by the code of a second embodiment.

[00065] Figure 5 illustrates the options for data content to be included in tokens in accordance with embodiments of the invention as described above.

[00066] Figure 6 provides a comparison of characteristics of embodiments of the present invention as compared with the prior art Swift-based messaging system.

[00067] Figure 7 is a block diagram in accordance with a further preferred embodiment of the present invention.

[00068] Figures 8A,8B and 8C are block diagrams of an implementation of a blockchain arrangement suitable for use with the system of embodiments of the invention,

[00069] Figure 9 is a block diagram in accordance with yet a further preferred embodiment of the present invention and

[00070] Figure 10 is a detailed block diagram of the system of figure 3C and figure 9.

2016901924 20 May 2016

DESCRIPTION OF EMBODIMENTS

[00071] With reference to Figure 1A there is illustrated in block form the basic components of a prior art settlement system. In many transactions there will be an at least first transacting entity 11 which enters into a transaction with an at least second transacting entity 12. The transaction may be as simple as the agreement by the first transacting entity 11 to sell a particular item or service to the second transacting entity 12. Typically the transaction will require settlement for an agreed amount expressed in a Fiat or other currency. In the vast majority of cases the at least first transacting entity 11 will be associated with an at least first intermediary entity 13, in this instance in the form of a bank A and similarly the second transacting entity 12 will be associated with an at least second intermediary entity 14 in this instance in the form of bank B. The first transacting entity 11 will have a first bank account 15 at the first intermediary entity 13 whilst second transacting entity 12 will have a second bank account 16 at second intermediary entity 14. Settlement of any given transaction requires instruction given by first transacting entity 11 to its first intermediary entity 13 to pay an agreed amount from the first bank account 15 to the bank account comprising second bank account 16 of second intermediary entity 14 of second transacting entity 12. For these instructions to be carried out metadata in the form of payment metadata 17 must be assembled at the first intermediary entity 13 sufficient and exhaustive to communicate to the second intermediary entity 14 such that the agreed settlement amount is transmitted from bank A to bank B and more particularly to the specific accounts of the respective first transacting entity 11 and second transacting entity 12.

[00072] A similar transaction may be applied in reverse where the second transacting entity sells a good or service to first transacting entity 11. In such an instance the respective intermediaries, once having received the respective payment metadata 17 and exchanged that metadata 17 may elect to simply pay the difference 18 electronically as between the intermediaries to effect the multiple transactions. In some instances, particularly where the transaction is cross-border-for example the first intermediary entity 13 is in a first country whilst the second intermediary entity 14 is in a second country the metadata 17 may include what is known as a Swift code which is a substantially unique identifier for each intermediary entity involved in the transaction. However, for any given transaction, far more data than merely a unique identifier for each intermediary entity involved in a transaction is required in order for the appropriate settlement amounts to ultimately be recorded in the correct accounts and settle the transaction for the agreed amounts.

2016901924 20 May 2016

[00073] Figure 1B is a data and funds flow diagram of data and funds flow according to a prior art settlement system at the granular level. In this instance, with reference to figure 1B like components are numbered as for figure 1A a given transaction requiring settlement can be embodied as a bill 90 which will include payment data 91 and may include bank facilitation payment data 92 comprising, in this instance, a biller code and a transaction code. Banks which are party to this bank facilitation payment system permit data entry by entity B (or payer B) 12 into a database of bank B 14 by means of a bank application or web interface 14 B. Bank B may then add additional data to form metadata 17 which is sent to a third-party server 93 which utilises metadata 17 to trigger pay (settlement) of bill 90 from payer B bank 14 to biller A bank 13.

Generalised Embodiment:

[00074] With reference to Figure 2C there is illustrated a block diagram of the basic infrastructure and components suited for use with embodiments of the present invention. In this instance like components are numbered as for figure 1 except in the 100 series. So, for example, first transacting entity 11 becomes first transacting entity 111 in this embodiment with reference to figure 2C.

[00075] In this instance a settlement system 110 according to a generalised embodiment includes at least first transacting entity 111 which enters into a transaction with at least a second transacting entity 112. As previously these entities are associated with a respective first intermediary entity 113 and a second intermediary entity 114 in the form of bank A and bank B. Each of the first transacting entity 111 and a second transacting entity 112 has a respective account 115, 116 at their respective intermediary entities as illustrated in figure 2C

[00076] In this instance, in the event that first transacting entity 111 enters into a transaction with second transacting entity 112 then, at the time of entry into the transaction 120, a token 121 is generated. In this instance the token 121 is generated by at least first digital device 122 communicating with a token database 123. The token database 123 generates a token comprising a data file 124 containing all data that will ultimately be required to settle the transaction 120 including any necessary identifying information for the transacting entity is, their accounts and the intermediary entities. Settlement is effected by communication of the token 121 to bank A and then to bank B together with the appropriate flow of funds.

2016901924 20 May 2016

[00077] With reference to figure 2A at the granular level a bill 190 from a biller 111 directed to a payer 112 contains bill data 191 and also token data of a token 121 residing within a code symbol 194 (in this instance a QR code). The token data includes pointer data pointing to data 195 on token database 123. The data 195 combined with bank ID data 114 permits the creation by token database 123 of a full payment record 196 which can be utilised to cause settlement of the bill 190 as against payer 112 via, in this instance, their respective banks 114, 113.

[00078] With reference to figure 2B the payment data record 196 is utilised has fed into a settlement network such as, for example a network 197 operating under the Ripple protocol thereby permitting substantially real-time settlement across multiple institutions and banks.

First Embodiment:

[00079] With reference to Figures 3 there is illustrated in block diagram form a first preferred embodiment of the present invention by way of a non-limiting example of a transaction. In this embodiment like components are numbered as for the previous embodiments except in the 200 series. So, for example, token 121 becomes token 221.

[00080] With reference to figure 3A the transaction system 210 is activated, as for the previous embodiment, when a transaction 220 is entered into between at least first transacting entity 211 and at least a second transacting entity 212 each dealing, for the purposes of this transaction, through respective intermediary entities 213, 214.

[00081] At the time of and as part of entry into the transaction 220 the first transacting entity 211 accesses token database 223 via digital device 222 executing via a web browser interface or via execution of an application running on a portable digital devices such as a mobile telephone or in a further alternative as a point-of-sale terminal in order to arrange for the database 223 to generate a token 221. In this instance the token 221 will include better data 224 including the recipient named, BIC, IBAN, destination country, mobile number, currency, business type, communication, payment amount. In this instance the token 221 including the metadata 224 is stored in the token database 223. In addition the first transacting entity 211 communicates the token 221 to a digital device 230 associated with second transacting entity 212. In this instance the communication is by way of initial transmission of the token 221 to digital device 222 which then on transmits the token via Internet 231 to digital device 230.

2016901924 20 May 2016

[00082] With reference to figure 3B, when ready to settle the transaction 220 the second transacting entity 212 "logs in" to a portal associated with second intermediary entity 214 and communicates the token 221. In this instance have the login can be executed via a web browser associated with digital device 230 which communicates via Internet 231 the token 221 to a digital processing system 232 (including at least a processor and a memory) associated with second intermediary entity 214. Substantially at the same time as part of seeking to settle the transaction 220:

[00083] Notification: token database 223 notifies second intermediary entity 214 to contact the token database 223 from which it receives a further token 221A.

[00084] Verification: token database 223 communicates with the processing system 232 of second intermediary entity 214 to verify that sufficient funds are located in account 216 as indicated in the meta data 224 to settle the transaction.

[00085] Committing payer funds: payers bank debits payers account: payers bank sends notice to payer bank gateway: payers bank gateway calls token database 223 to get approved token:

[00086] Settlement: gateway of payers bank sends by way of non-limiting example XRP (the native currency of the Ripple protocol) to billers bank gateway: payers bank gateway notifies token database 223 of receipt:

[00087] Clearing: payer's bank Nostro account is debited subject to bank institution rules.

[00088] Embodiments of the invention can be implemented utilising the "Ripple" the framework, protocol and gateway-or more generally any blockchain based framework. In a particular form the final settlement process can be enabled through a Ripple frame work thereby to facilitate substantially real-time settlement across multiple institutions and multiple banks.

Second Embodiment:

[00089] Examples of tokenised messages and their generation and transmission are illustrated in pseudocode below. Reference to "sparro" is a reference to an instance of a token database123.

[00090] The previous, meta-data mode is first. It switches to minimal half way through

--

2016901924 20 May 2016

Bank:HSBC >> createUserCode >> Sparro:Sparro

{"id":"User:ABC Paper","name":"ABC Paper"}

(Creating Sparro User Code - Meta-data given can be used by other banks for compliance and for confirming payee with customers.)

--

Bank:MayBank >> createUserCode >> Sparro:Sparro

{"id":"User:XYZ Printing","name":"XYZ Printing"}

(Creating Sparro User Code - Meta-data given can be used by other banks for compliance and for confirming payee with customers.)

--

Sparro:Sparro >> createUserCode-reply >> Bank:HSBC

{"id":"User:ABC Paper","name":"ABC Paper","code":"65q3gdd"}

--

Sparro:Sparro >> createUserCode-reply >> Bank:MayBank

{"id":"User:XYZ Printing","name":"XYZ Printing","code":"70wqgx6"}

--

User:ABC Paper >> createInvoice >> Bank:HSBC

{"amount":{"amount":1000,"currency":"gbp"}}

--

Bank:HSBC >> createInvoiceCode >> Sparro:Sparro

{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd"}

(Creating Invoice Code - An invoice code is created by Sparro and connected to the bank.)

-

Sparro:Sparro >> createInvoiceCode-reply >> Bank:HSBC

{"code":"6tq6wcbad"}

--

Bank:HSBC >> createInvoice-reply >> User:ABC Paper

{"invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

2016901924 20 May 2016

Abc invoice { amount: { amount: 1000, currency: 'gbp' },
payee: '65q3gdd',
code: '6tq6wcbad' }

--

User:ABC Paper >> invoice >> User:XYZ Printing

{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}

-

User:XYZ Printing >> payInvoice >> Bank:MayBank

{"invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300}}

--

Bank:MayBank >> sendMoney >> BankGateway:MayBank

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300}}

--

BankGateway:MayBank >> getInvoice >> Sparro:Sparro

"6tq6wcbad"

(Sending Payment to Invoice - The payment is sent to the bank that created the invoice.)

--

Sparro:Sparro >> getInvoice-reply >> BankGateway:MayBank

{"bank":"Bank:HSBC","invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

--

BankGateway:MayBank >> transfer >> BankGateway:HSBC

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":"ripple-1"}

--

BankGateway:HSBC >> incomingTransfer >> Bank:HSBC

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":"ripple-1"}

--

20 May 2016 2016901924

BankGateway:HSBC >> transfer-reply >> BankGateway:MayBank

{"success":true,"owed":{"GBP":300}}

--

Bank:HSBC >> getInvoice >> Sparro:Sparro

"6tq6wcbad"

--

BankGateway:MayBank >> sendMoney-reply >> Bank:MayBank

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":"ripple-1"}

--

Sparro:Sparro >> getInvoice-reply >> Bank:HSBC

{"bank":"Bank:HSBC","invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

--

Bank:MayBank >> payInvoice-reply >> User:XYZ Printing

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":"ripple-1"}

XYZ part-paid invoice {

"payer": "70wqgx6",
"invoice": "6tq6wcbad",
"amount": {
"currency": "GBP",
"amount": 300
},
"id": "ripple-1"

}

--

2016901924 20 May 2016

Bank:HSBC >> incomingTransfer >> User:ABC Paper

{"invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"},"transfer":{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":"ripple-1"}}

-

User:XYZ Printing >> payInvoice >> Bank:MayBank

{"invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700}}

--

Bank:MayBank >> sendMoney >> BankGateway:MayBank

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700}}

--

BankGateway:MayBank >> getInvoice >> Sparro:Sparro

"6tq6wcbad"

(Sending Payment to Invoice - The payment is sent to the bank that created the invoice.)

--

Sparro:Sparro >> getInvoice-reply >> BankGateway:MayBank

{"bank":"Bank:HSBC","invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

--

BankGateway:MayBank >> transfer >> BankGateway:HSBC

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700},"id":"ripple-2"}

--

2016901924 20 May 2016

BankGateway:HSBC >> incomingTransfer >> Bank:HSBC

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700},"id":"ripple-2"}

--

BankGateway:HSBC >> transfer-reply >> BankGateway:MayBank

{"success":true,"owed":{"GBP":1000}}

--

Bank:HSBC >> getInvoice >> Sparro:Sparro

"6tq6wcbad"

-

BankGateway:MayBank >> sendMoney-reply >> Bank:MayBank

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700},"id":"ripple-2"}

--

Sparro:Sparro >> getInvoice-reply >> Bank:HSBC

{"bank":"Bank:HSBC","invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

--

Bank:MayBank >> payInvoice-reply >> User:XYZ Printing

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700},"id":"ripple-2"}

XYZ finished paying invoice {

"payer": "70wqgx6",
"invoice": "6tq6wcbad",

20 May 2016 2016901924


```
 "amount": {
  "currency": "GBP",
  "amount": 700
 },
 "id": "ripple-2"
}
```


--- SWITCHING TO MODE: minimal ---

--

Bank:HSBC >> incomingTransfer >> User:ABC Paper


```
{"invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcb
ad"},"transfer":{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amo
unt":700},"id":"ripple-2"}}
```


--Bank:HSBC >> createUserCode >> Sparro:Sparro

undefined

(Creating Sparro User Code - No meta-data is required.)

--

Bank:MayBank >> createUserCode >> Sparro:Sparro

undefined

(Creating Sparro User Code - No meta-data is required.)

--

Sparro:Sparro >> createUserCode-reply >> Bank:HSBC


```
{"code":"dnt7gec"}
```


--

Sparro:Sparro >> createUserCode-reply >> Bank:MayBank


```
{"code":"6wwpwuc"}
```

2016901924 20 May 2016

--

User:ABC Paper >> createInvoice >> Bank:HSBC

{"amount":{"amount":2000,"currency":"gbp"}}

--

Bank:HSBC >> createInvoiceCode >> Sparro:Sparro

null

(Creating Invoice Code - An invoice code is created by Sparro and connected to the bank. No invoice details are required.)

--

Sparro:Sparro >> createInvoiceCode-reply >> Bank:HSBC

{"code":"erwkax1md"}

--Bank:HSBC >> createInvoice-reply >> User:ABC Paper

{"invoice":{"amount":{"amount":2000,"currency":"gbp"},"code":"erwkax1md","payee":"User:ABC Paper","transfers":[]}}

Abc invoice { amount: { amount: 2000, currency: 'gbp' },
code: 'erwkax1md',
payee: 'User:ABC Paper',
transfers: [] }

--

User:ABC Paper >> invoice >> User:XYZ Printing

{"amount":{"amount":2000,"currency":"gbp"},"code":"erwkax1md","payee":"User:ABC Paper","transfers":[]}

--

User:XYZ Printing >> payInvoice >> Bank:MayBank

{"invoice":"erwkax1md","amount":{"currency":"GBP","amount":600}}

2016901924 20 May 2016

--

Bank:MayBank >> sendMoney >> BankGateway:MayBank

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600}}

--

BankGateway:MayBank >> getInvoice >> Sparro:Sparro

"erwkax1md"

(Sending Payment to Invoice - The payment is sent to the bank that created the invoice.)

--

Sparro:Sparro >> getInvoice-reply >> BankGateway:MayBank

{"bank":"Bank:HSBC"}

--

BankGateway:MayBank >> transfer >> BankGateway:HSBC

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}

--

BankGateway:HSBC >> incomingTransfer >> Bank:HSBC

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}

--

BankGateway:HSBC >> transfer-reply >> BankGateway:MayBank

{"success":true,"owed":{"GBP":600}}

--

Bank:HSBC >> incomingTransfer >> User:ABC Paper

{"invoice":{"amount":{"amount":2000,"currency":"gbp"},"code":"erwkax1md","payee":"User:ABC

Paper","transfers":[{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP"

2016901924 20 May 2016

,"amount":600},"id":"ripple-
3"}]},"transfer":{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","a
mount":600},"id":"ripple-3"}}

--

BankGateway:MayBank >> sendMoney-reply >> Bank:MayBank

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id
":"ripple-3"}

--

Bank:MayBank >> payInvoice-reply >> User:XYZ Printing

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id
":"ripple-3"}

XYZ part-paid invoice {
 "payer": "6wwpwuc",
 "invoice": "erwkax1md",
 "amount": {
  "currency": "GBP",
  "amount": 600
 },
 "id": "ripple-3"
}

--

User:XYZ Printing >> payInvoice >> Bank:MayBank

{"invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400}}

--

Bank:MayBank >> sendMoney >> BankGateway:MayBank

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400}}

2016901924 20 May 2016

--

BankGateway:MayBank >> getInvoice >> Sparro:Sparro

"erwkax1md"

(Sending Payment to Invoice - The payment is sent to the bank that created the invoice.)

--

Sparro:Sparro >> getInvoice-reply >> BankGateway:MayBank

{"bank":"Bank:HSBC"}

-

BankGateway:MayBank >> transfer >> BankGateway:HSBC

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}

--

BankGateway:HSBC >> incomingTransfer >> Bank:HSBC

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}

BankGateway:HSBC >> transfer-reply >> BankGateway:MayBank

{"success":true,"owed":{"GBP":2000}}

--

Bank:HSBC >> incomingTransfer >> User:ABC Paper

{"invoice":{"amount":{"amount":2000,"currency":"gbp"},"code":"erwkax1md","payee":"User:ABC
Paper","transfers":[{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-
3"},{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-

20 May 2016 2016901924

4"}]},"transfer":{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}}

--

BankGateway:MayBank >> sendMoney-reply >> Bank:MayBank

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}

--

Bank:MayBank >> payInvoice-reply >> User:XYZ Printing

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}

XYZ finished paying invoice {

"payer": "6wwpwuc",
"invoice": "erwkax1md",
"amount": {
"currency": "GBP",
"amount": 1400
},
"id": "ripple-4"

}

features of this embodiment include the enablement of a private, invitation only, network for banking institutions which, in a particular form, can facilitate cross-border payments thereby to enable substantially real-time payments at reduced processing cost.

[00091] With reference to figure 4 there is shown a block diagram of salient characteristics of a messaging system 10 of the prior art as compared with the salient messaging characteristics of the system 210 enabled by the code listed above and more broadly described with reference to the earlier embodiments.

2016901924 20 May 2016

[00092] Figure 5 illustrates the options for data content to be included in tokens in accordance with embodiments of the invention as described above.

[00093] Figure 6 provides a comparison of characteristics of embodiments of the present invention as compared with the prior art Swift-based messaging system at a commercial layer 470, a security layer 471 and a technical layer 472.

Further Embodiment

[00094] Figure 7 is a block diagram of a further embodiment. In this instance a distributed ledger 781 operating on blockchain principles provides for transmission of the tokenised message as for previous embodiments.

[00095] In this instance it will be observed that the tokenised transmission distributed ledger 781 operates in parallel with conventional transmission between institution A and institution B.

[00096] Conventional transmission includes transmission of conventional messages utilising the SWIFT protocol. It is also to be noted that institution A and institution B may be subsidiaries of the same institution or may otherwise be closely related. In the alternative they may be completely independent institutions.

[00097] The tokenised message as described in previous embodiments may include information as typically transmitted by the SWIFT or other current acknowledged data transmission systems for transmission of financial information for the purpose of transfer of funds between parties.

[00098] The tokenised message may transmit data which includes some of the data normally included in the conventional message. In alternative forms it may include additional data. In yet alternative forms it may include data not transferred at all in the data normally included in the conventional message.

[00099] The aim, in particular forms, ultimately, is to improve the reliability of the transaction as between the first transacting entity and the second transacting entity and, in some forms, to provide an enhanced capability.

[000100] In the arrangement of figure 7 the data comprising the tokenised message is transmitted via nodes 780 within a blockchain 781.

2016901924 20 May 2016

[000101] In summary, Bank A and Bank B might be branches of the same bank, say HSBC HK and HSBC China (which today use SWIFT for intrabank transfers). So this system could be used within 1 financial institution.

[000102] In one form the purpose of storing the token only in the blockchain is really to both de-identify the information in the blockchain (which is critical for banks), and enable use of existing (SWIFT / ACH / RTGS) or new messaging systems to send the payment instruction in tokenised format. Banks today have significant investment in existing conventional messaging systems and a complete abandonment of these messaging systems would not be feasible. However settlement is still a manual process so linking the conventional messaging system to the 'blockchain' settlement system (via the token) is an important feature of this embodiment. So, in diagram 7 we include a SWIFT/ACH/RTGS connection between the two Financial Institutions (FIs) (or branches) for communication of the token, and the blockchain ledger is common. The data that is required to settle the payment can be provided by the FI's customer or by the FI themselves (say from a core banking system or similar).

[000103] Fig 8 illustrates in block diagram form key components of an implementation of a blockchain structure which may be utilised to implement the system of figure 7.

[000104] Each block includes verified transactions and the blockchain maintains a ledger all prior transactions. The blockchain is duplicated by all the computers on a network.

[000105] The first block in the chain is known as the Genesis block and new blocks can be added in linear and chronological order. From any given block in the chain the information of this genesis block and all blocks that led back to this one can be retrieved. A blockchain is essentially numerous blocks connected through hash chaining where each block is comprised of the following (see figure 8);

- Timestamp: provides proof that the data in a block existed at a particular time
- Previous Hash: Essentially a pointer to the previous block
- Merkle Hash: Summary of all executed transactions
- Nonce: Individual blocks identity and is an arbitrary number which can only be used once

2016901924 20 May 2016

[000106] The blockchain is managed by a network of distributed nodes where each node contains a copy of the entire blockchain. Each node in the network can add blocks to the chain, where every node is adding blocks at the same point in the chain at the same time. The more nodes that comprise the network the harder it is to disrupt the storage of the blockchain. Unlike centralised systems which rely on a single authority, there is no single point of failure in these distributed nodes network. If you change the content of a block you change its Hash.

[000107] Blockchains can be based on/ operate in association with any one of a number of protocols – for example Ripple or Stellar.

[000108] Figure 8B shows a first step in creation of records in the block chain structure of figure 8A whilst figure 8C shows a second step in the creation of records in the chain structure of figure 8A. The chain structures of this type may be utilised in relation to the embodiments described in this application.

Yet further embodiment

[000109] Figure 9 is a block diagram of a further embodiment wherein the parallel data transmission capabilities of the system are further detailed as compared with the embodiment of figure 7. Components are numbered as for previous embodiments except in the 800 series. So, for example, first transacting entity 711 of the further embodiment of figure 7 becomes the first transacting entity 811. In this instance a distributed ledger 881 operating on blockchain principles (refer description with reference to figure 8) provides for transmission of the tokenised message as for previous embodiments.

[000110] In this instance it will be observed that the tokenised transmission distributed ledger 881 operates in parallel with conventional transmission between institution A and institution B.

[000111] Conventional transmission includes transmission of conventional messages utilising the SWIFT protocol. It is also to be noted that institution A 813 and institution B 814 may be subsidiaries of the same institution or may otherwise be closely related. In the alternative they may be completely independent institutions.

[000112] The tokenised message 890 as described in previous embodiments may include information as typically transmitted by the SWIFT or other current acknowledged data transmission

2016901924 20 May 2016

systems for transmission of financial information for the purpose of transfer of funds between parties.

[000113] The tokenised message may transmit data which includes some of the data normally included in the conventional message. In alternative forms and more particularly the form with reference to figure 9 it may include additional data however, in this instance the additional data 891 is transmitted via blockchain 881 as an entry in a shared ledger 892. The additional data 891 in this instance comprises a token value 893, a transaction value 894 a sender cheque status flag 895 and a token state 896. This entry 897 in shared ledger 892 can be accessed based on token value 893. In an alternative form the entry 897 and more particularly the token value 893 may be secured for example requiring a separate key before the data can be accessed and/or decrypted. The data in entry 897 may comprise deidentified data thereby to ensure that no personally identifiable information is transmitted to Bank (second intermediary entity 814).

[000114] The aim, ultimately, is to improve the reliability of the transaction as between the first transacting entity and the second transacting entity and, in some forms, to provide an enhanced capability.

[000115] In particular, in preferred forms an element includes provision of systems which add additional information whereby the additional information is to enrich payments with more information given the inability of existing payment systems to communicate enriched information.

[000116] In the arrangement of figure 9 the data comprising the tokenised message is transmitted via nodes 880 within a blockchain 881.

[000117] In summary, Bank A and Bank B might be branches of the same bank, say HSBC HK and HSBC China (which today use SWIFT for intrabank transfers). So this system could be used within 1 financial institution.

[000118] In one form the purpose of storing the token only in the blockchain is really to both de-identify the information in the blockchain (which is critical for banks), and enable use of existing (SWIFT / ACH / RTGS) or new messaging systems to send the payment instruction in tokenised format. Banks today have significant investment in existing conventional messaging systems and a complete abandonment of these messaging systems would not be feasible. However settlement is still a manual process so linking the conventional messaging system to the 'blockchain' settlement system (via the token) is an important feature of this embodiment. So, in figure 9 we include a

2016901924 20 May 2016

SWIFT/ACH/RTGS connection between the two Financial Institutions (FIs) (or branches) for communication of the token, and the blockchain ledger is common. The data that is required to settle the payment can be provided by the FI's customer or by the FI themselves (say from a core banking system or similar).

[000119] Figure 10 is a detailed block diagram of the system of figure 3C and figure 9.

[000120] With reference to Figure 10 there is illustrated in block diagram form a first preferred embodiment of the present invention by way of a non-limiting example of a transaction. In this embodiment like components are numbered as for Figure 9 in the 800 series.

[000121] With reference to figure 10 the transaction system 210 is activated, as for the previous embodiment, when a transaction 220 is entered into between at least first transacting entity 211 and at least a second transacting entity 212 each dealing, for the purposes of this transaction, through respective intermediary entities 213, 214.

[000122] At the time of and as part of entry into the transaction 220 the first transacting entity 211 accesses token database 223 via digital device 222 executing via a web browser interface or via execution of an application running on a portable digital devices such as a mobile telephone or in a further alternative as a point-of-sale terminal in order to arrange for the database 223 to generate a token 221. In this instance the token 221 will include better data 224 including the recipient named, BIC, IBAN, destination country, mobile number, currency, business type, communication, payment amount. In this instance the token 221 including the metadata 224 is stored in the token database 223. In addition the first transacting entity 211 communicates the token 221 to a digital device 230 associated with second transacting entity 212. In this instance the communication is by way of initial transmission of the token 221 to digital device 222 which then on transmits the token via Internet 231 to digital device 230.

[000123] With reference to figure 10, when ready to settle the transaction 220 the second transacting entity 212 "logs in" to a portal associated with second intermediary entity 214 and communicates the token 221. In this instance have the login can be executed via a web browser associated with digital device 230 which communicates via Internet 231 the token 221 to a digital processing system 232 (including at least a processor and a memory) associated with second

2016901924 20 May 2016

intermediary entity 214. Substantially at the same time as part of seeking to settle the transaction 220:

[000124] Notification: token database 223 notifies second intermediary entity 214 to contact the token database 223 from which it receives a further token 221A.

[000125] Verification: token database 223 communicates with the processing system 232 of second intermediary entity 214 to verify that sufficient funds are located in account 216 as indicated in the meta data 224 to settle the transaction.

[000126] Committing payer funds: payers bank debits payers account: payers bank sends notice to payer bank gateway: payers bank gateway calls token database 223 to get approved token:

[000127] Settlement: gateway of payers bank sends by way of non limiting example XRP (the native currency of the Ripple protocol) to billers bank gateway: payers bank gateway notifies token database 223 of receipt:

[000128] Clearing: payer's bank may be a Nostro account which is debited subject to bank institution rules.

[000129] Embodiments of the invention can be implemented utilising the "Ripple" framework, protocol and gateway-or more generally any blockchain based framework. In a particular form the final settlement process can be enabled through a Ripple framework thereby to facilitate substantially real-time settlement across multiple institutions and multiple banks.

[000130] With further reference to figure 10 it will be observed that the token 221, in this instance, may be conveyed between bank 213 and bank 214 by way of a medium 260 utilizing the SWIFT protocol or other compatible protocols 250. In preferred forms the medium the medium will be an electronic communications medium and in particular forms may be implemented by way of a VPN established between bank 213 and bank 214.

[000131] Separately deidentified data 251 A, B, C, D associated with the transaction to which the token pertains may be transmitted over a separate communication medium, in this instance internet 231. In a preferred form the communication medium utilizes a blockchain structure as described earlier in this specification and the deidentified data 251 A, B, C, D is located within a record structure 261 which is replicated throughout the blockchain structure.

2016901924 20 May 2016

[000132] In use a sellers bank 213 as part of entering into the transaction with buyers bank 214 will establish a SWIFT transaction transmittable over medium 260. Separately and preferably in parallel the sellers bank 213 will perform associated operations needed to complete the transaction such as verification of the buyers ID and related characteristics. Data related to these associated operations is then placed in record structure 261 and that record is placed into the blockchain structure. The associated data includes deidentifed data 251 A, B, C, D.

[000133] This data is available to the buyers bank 214 by way of the buyers bank logging into the blockchain structure and receiving the deidentified data which is associated with the transaction which is represented by token 221. Thereby allowing assembly by the buyers bank 214 of all necessary data to execute the transaction on behalf of the buyer and seller.

[000134] With reference to figures 7 and 10 the system provides for communication of invoice/purchase order /remittance advice information as illustrated.

[000135] It will be further observed that blockchain structures may be utilized to provide an information layer above existing legacy systems (for example based on SWIFT protocols and the like) and wherein the additional information layer provides enriched information about payments using the token. It is to be noted that existing systems do not provide enriched information and, in more particular forms, do not provide deidentified information/data for use by the communicating parties.

[000136] The above describes only some embodiments of the present invention and modifications, obvious to those skilled in the art, can be made thereto without departing from the scope of the present invention.

2016901924 20 May 2016

CLAIMS

1. A system for settling a transaction electronically; said system comprising:
   a) at least a first transacting entity;
   b) at least a second transacting entity;
   c) at least a first intermediary entity;
   d) at least a second intermediary entity;
   e) in the case where the first transacting entity enters into a transaction with the second transacting entity generating a tokenised message at the time of the transaction containing data needed to settle the transaction;
   f) initiating settlement of the transaction by transmission of the tokenised message between at least two of the entities.
2. The system of claim 1 wherein the tokenised message is generated with reference to a token database located at a remote location.
3. The system of claim 2 wherein the tokenised message includes at least a first data element, a second data element and a third data element.
4. The system of claim 3 wherein the first data element comprises identification data for a payor, the second data element comprises identification data for a payee (biller) and the third data element comprises identification currency, denomination and value data.
5. The system of claim 1 or claim 2 wherein a further tokenised message is generated by either an intermediary entity or the token database.
6. The system of any previous claim wherein a tokenised message is generated by a bi-directional communication process.
7. The system of claim 6 wherein the bi-directional communication process is between the token database and an intermediary entity.
8. The system of any previous claim wherein a step in producing a tokenised message involves de-identifying data.
9. The system of any previous claim wherein a step in producing a tokenised message involves adding a data element to the message.
10. The system of any previous claim wherein a step in producing a tokenised message involves removing a data element from the message.
11. The system of any previous claim wherein a step in producing a tokenised message involves applying an algorithm to the data elements in the message.

2016901924 20 May 2016

12. The system of any previous claim wherein the token database sequences the tokenised messages.
13. The system of any previous claim wherein the token database sequences the tokenised messages and transmits the tokenised messages as payment data records to a blockchain ledger settlement system.
14. The system of claim 13 wherein the blockchain settlement system employs the Ripple protocol.
15. A tokenised message construction system; said system comprising:
    a) a server in communication with a database and which facilitates communications between a plurality of parties to a transaction;
    b) each party having a digitised device with which to communicate with other ones of the parties and with the server;
    c) each party capable of generating a tokenised message via a bidirectional communication with the server.
16. The system of claim 15 wherein the tokenised message is generated with reference to a token database located at a remote location.
17. The system of claim 16 wherein the tokenised message includes at least a first data element, a second data element and a third data element.
18. The system of claim 17 wherein the first data element comprises identification data for a payor, the second data element comprises identification data for a payee (biller) and the third data element comprises identification currency, denomination and value data.
19. The system of claim 15 or claim 16 wherein a further tokenised message is generated by either an intermediary entity or the token database.
20. The system of any one of claims 15 to 19 wherein a tokenised message is generated by a bi-directional communication process.
21. The system of claim 20 wherein the bi-directional communication process is between the token database and an intermediary entity.
22. The system of any one of claims 15 to 21 wherein a step in producing a tokenised message involves de-identifying data.
23. The system of any one of claims 15 to 22 wherein a step in producing a tokenised message involves adding a data element to the message.
24. The system of any one of claims 15 to 23 wherein a step in producing a tokenised message involves removing a data element from the message.

2016901924 20 May 2016

25. The system of any one of claims 15 to 24 wherein a step in producing a tokenised message involves applying an algorithm to the data elements in the message.
26. The system of any one of claims 15 to 25 wherein the token database sequences the tokenised messages.
27. The system of any one of claims 15 to 26 wherein the token database sequences the tokenised messages and transmits the tokenised messages as payment data records to a blockchain settlement system.
28. The system of claim 27 wherein the blockchain settlement system employs the Ripple protocol.
29. The system of any previous claim wherein a second message is transmitted between the intermediaries.
30. The system of claim 29 wherein the second message is tokenised.
31. The system of claim 29 or 30 wherein the second message contains conventional data.
32. The system of claim 29 or 30 or 31 wherein the second message is transmitted by means of a blockchain system.
33. The system of claim 29 or 30 or 31 wherein the second message includes information equivalent to that transmitted by the SWIFT system.
34. The system of claim 29 or 30 or 31 wherein the tokenised message includes additional information beyond that transmitted by the SWIFT system.
35. The system of claim 35 wherein the tokenised message includes information which verifies the security status of at least one party to the transaction.
36. The system of claim 35 wherein the second tokenised message includes information which verifies the security status of both parties to the transaction.
37. The system of any previous claim wherein the token is conveyed by way of a medium utilizing the SWIFT messaging system or other compatible messaging system.
38. The system of claim 37 wherein the medium is implemented by way of a VPN.
39. The system of any previous claim wherein deidentified data associated with the transaction to which the token pertains is transmitted over a separate communication medium.
40. The system of claim 9 wherein the separate communication medium utilizes a blockchain structure.
41. The system of claim 39 or 40 wherein the deidentified data is located within a record structure which is replicated throughout the blockchain structure.

2016901924 20 May 2016

42. The system of any previous claim wherein in use a sellers bank as part of entering into the transaction with buyers bank will establish a SWIFT transaction.

43. The system of claim 42 wherein in parallel the sellers bank will perform associated operations needed to complete the transaction such as verification of the buyers ID and related characteristics.

44. The system of claim 43 wherein data related to the associated operations is then placed in a record structure and that record is placed into the blockchain structure.

45. The system of claim 44 wherein the associated data includes deidentifed data.

46. The system of any one of claims 42 to 45 wherein the data is available to the buyers bank by way of the buyers bank logging into the blockchain structure and receiving the deidentified data which is associated with the transaction which is represented by the token thereby allowing assembly by the buyers bank of all necessary data to execute the transaction on behalf of the buyer and seller.

47. The system of any previous claim incorporating secure channels thereby permitting only selected entities to communicate the data to execute the transaction on behalf of the buyer and seller.

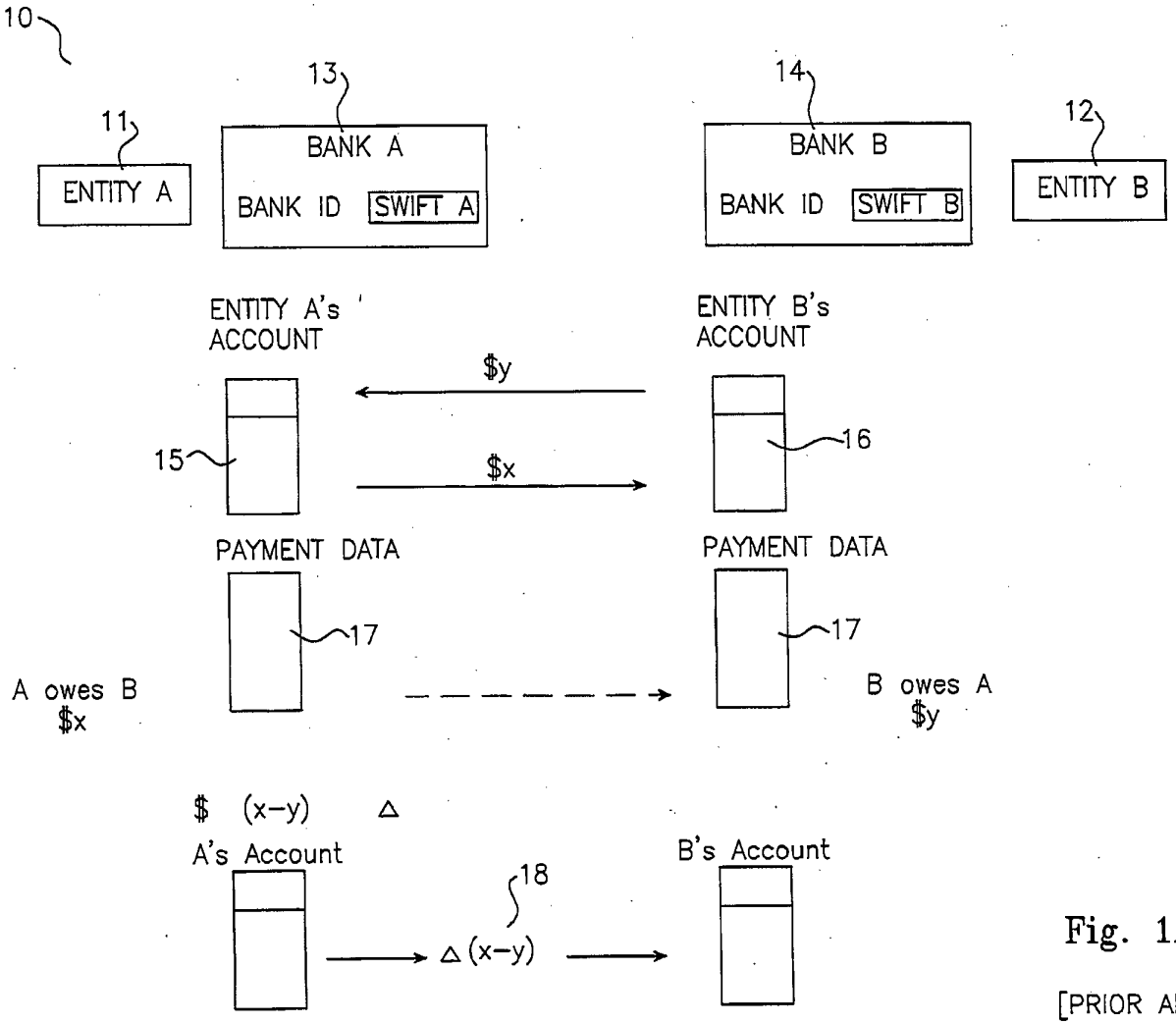
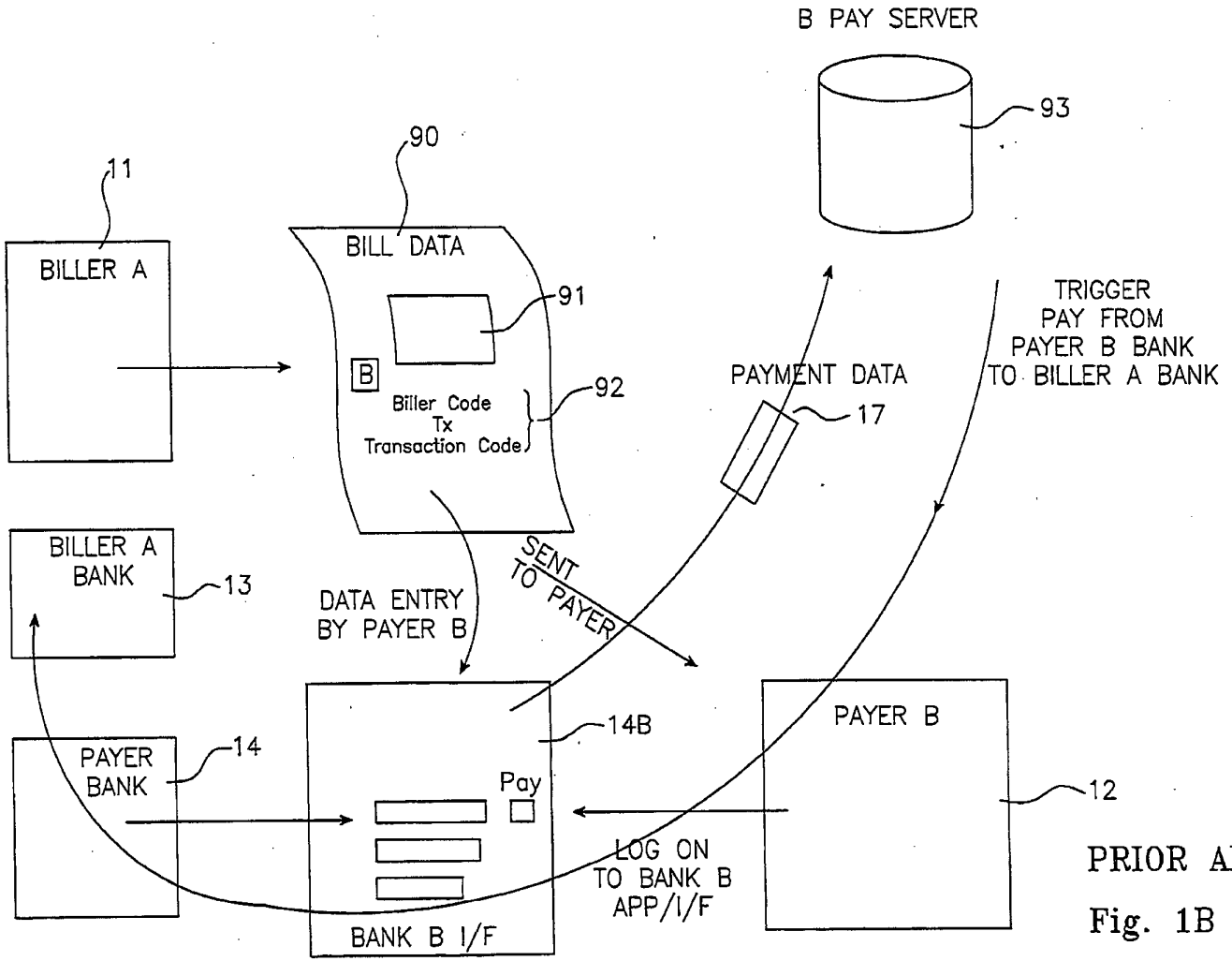


Fig. 1A

[PRIOR ART]

1/16



PRIOR ART

Fig. 1B

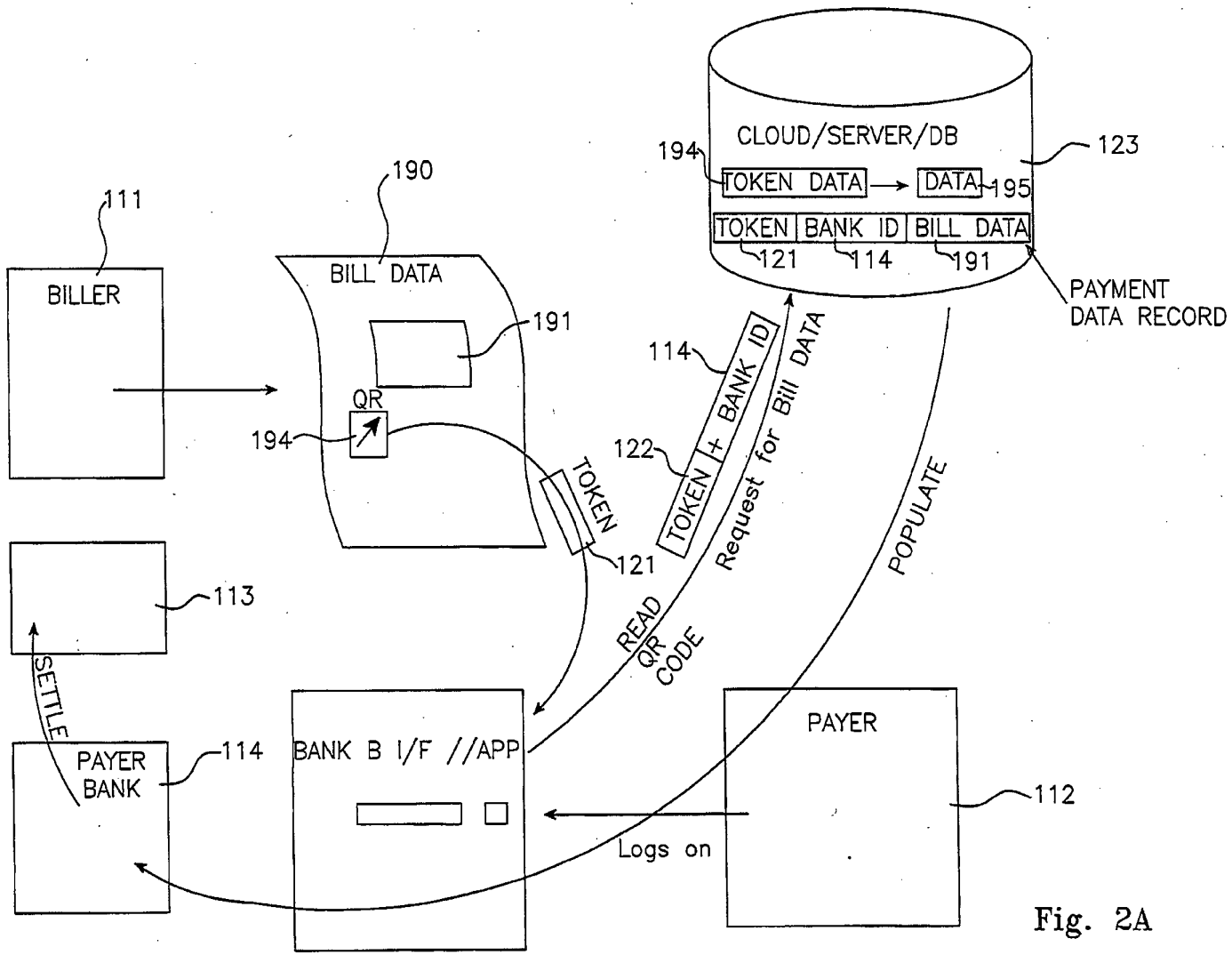

CLOUD/SERVER/DB
123
194
TOKEN DATA
DATA
195
TOKEN
BANK ID
BILL DATA
121
114
191
PAYMENT DATA RECORD
111
BILLER
190
BILL DATA
191
QR
194
TOKEN
121
114
BANK ID
122
TOKEN
Request for Bill DATA
POPULATE
READ QR CODE
113
SETTLE
PAYER BANK
114
BANK B I/F //APP
PAYER
112
Logs on

Fig. 2A

3/16

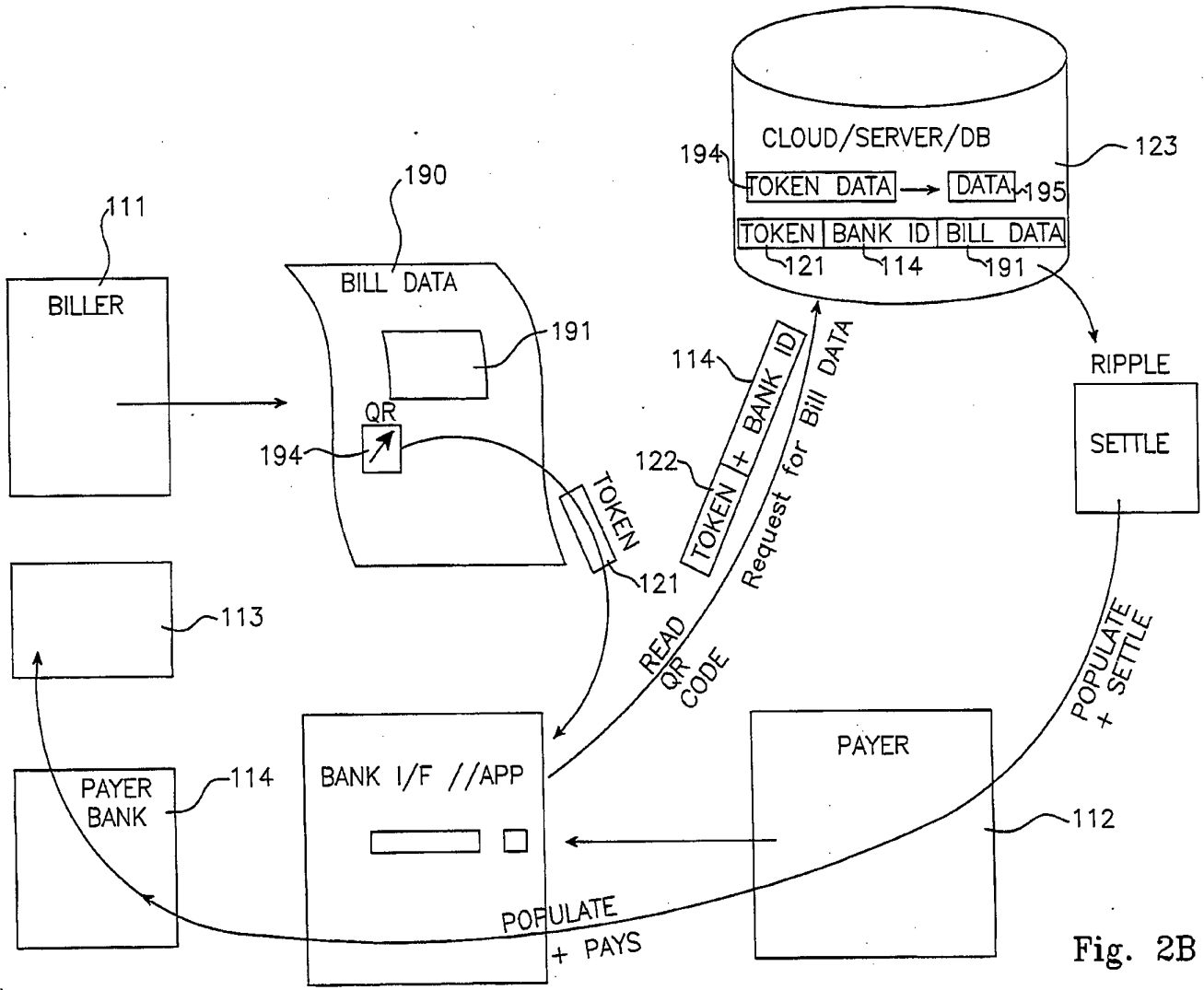

CLOUD/SERVER/DB
123
194
TOKEN DATA
DATA
195
TOKEN
BANK ID
BILL DATA
121
114
191
111
BILLER
190
BILL DATA
191
QR
194
TOKEN
121
114
BANK ID
122
TOKEN
Request for Bill DATA
RIPPLE
SETTLE
113
READ QR CODE
POPULATE + SETTLE
PAYER BANK
114
BANK I/F //APP
PAYER
112
POPULATE + PAYS

Fig. 2B

4/16

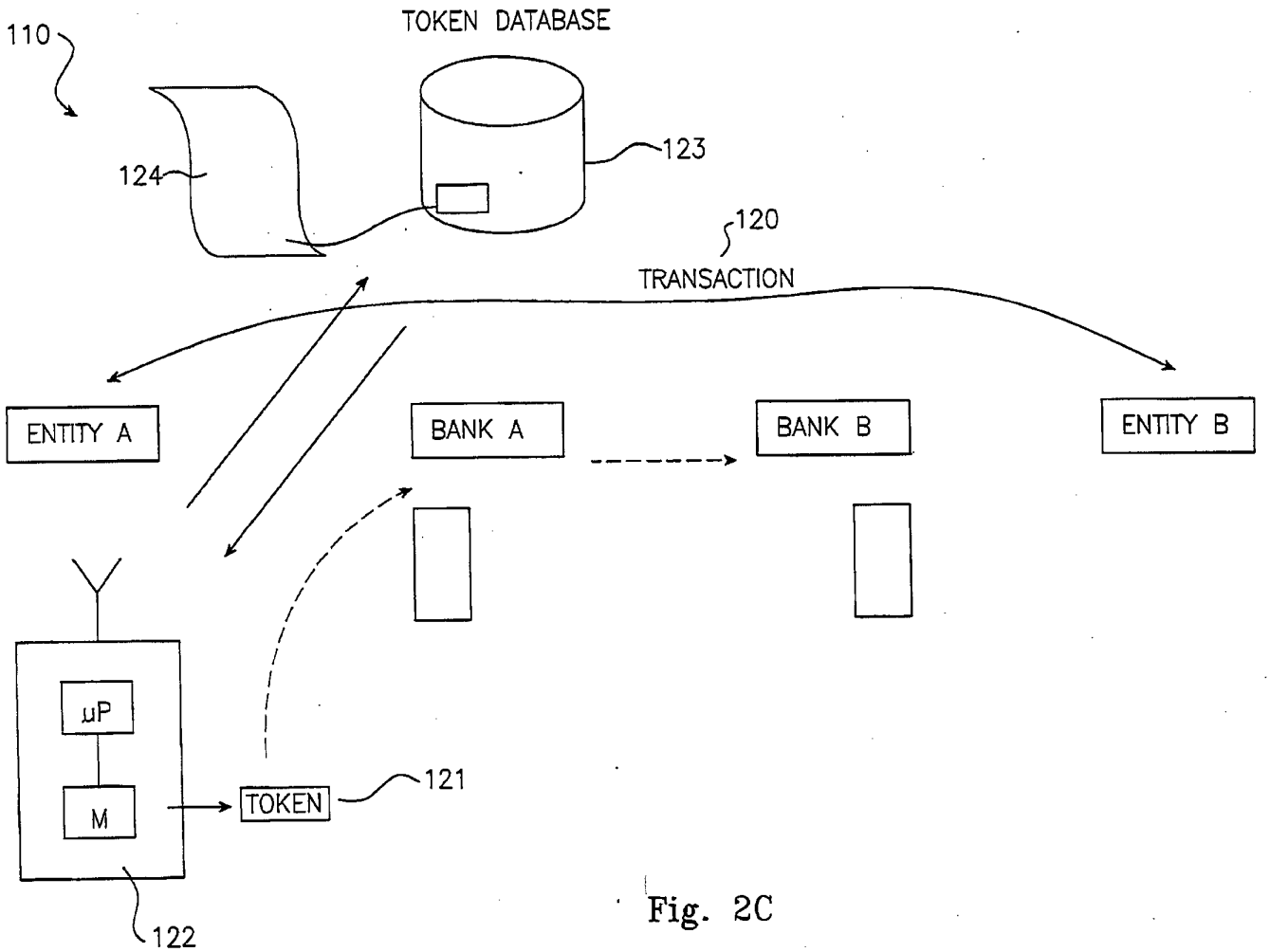

110
TOKEN DATABASE
123
124
120
TRANSACTION
ENTITY A
BANK A
BANK B
ENTITY B
μP
M
TOKEN
121
122

Fig. 2C

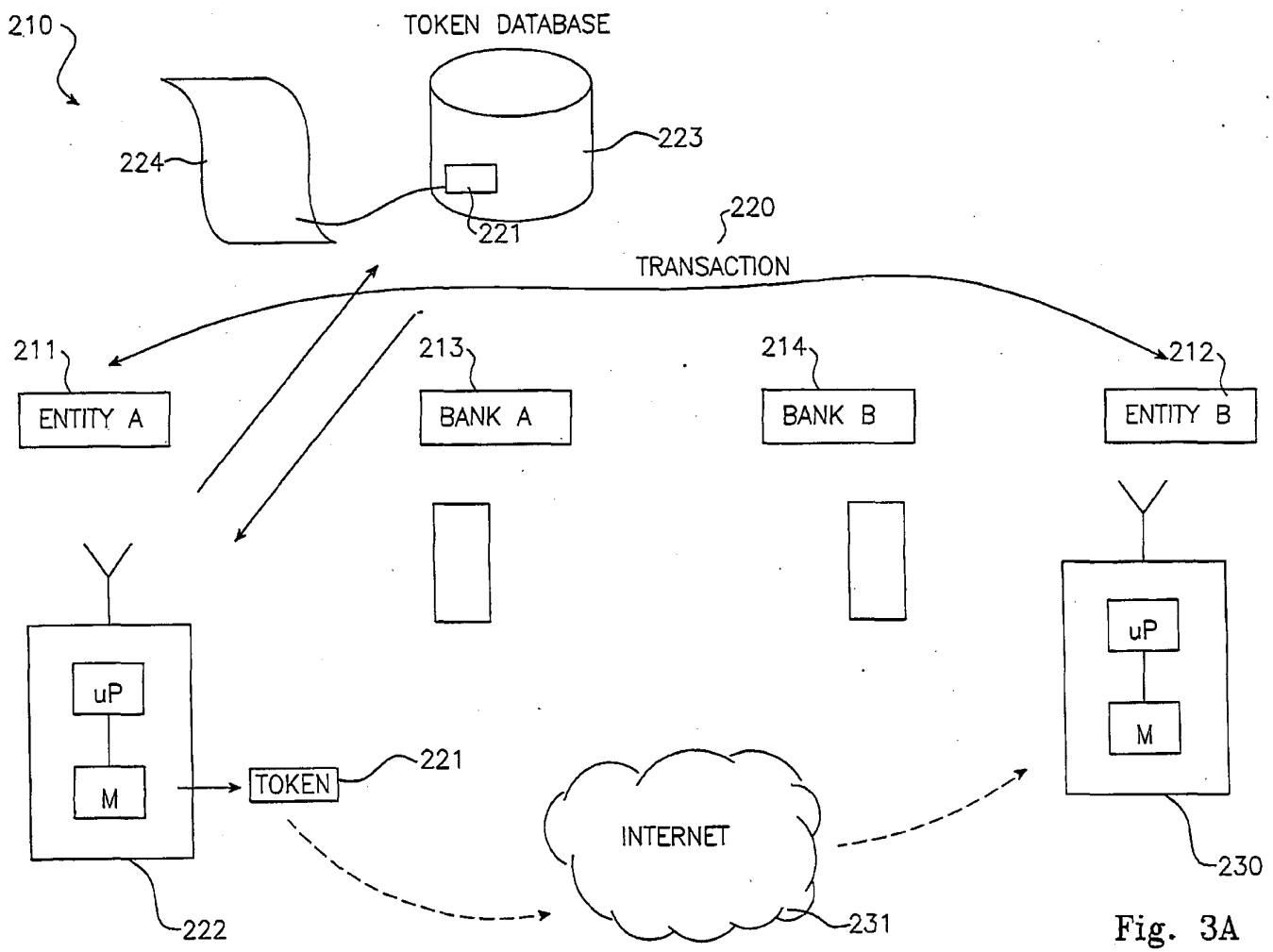

210
TOKEN DATABASE
223
224
221
220
TRANSACTION
211
213
214
212
ENTITY A
BANK A
BANK B
ENTITY B
uP
M
TOKEN
221
INTERNET
uP
M
230
222
231

Fig. 3A

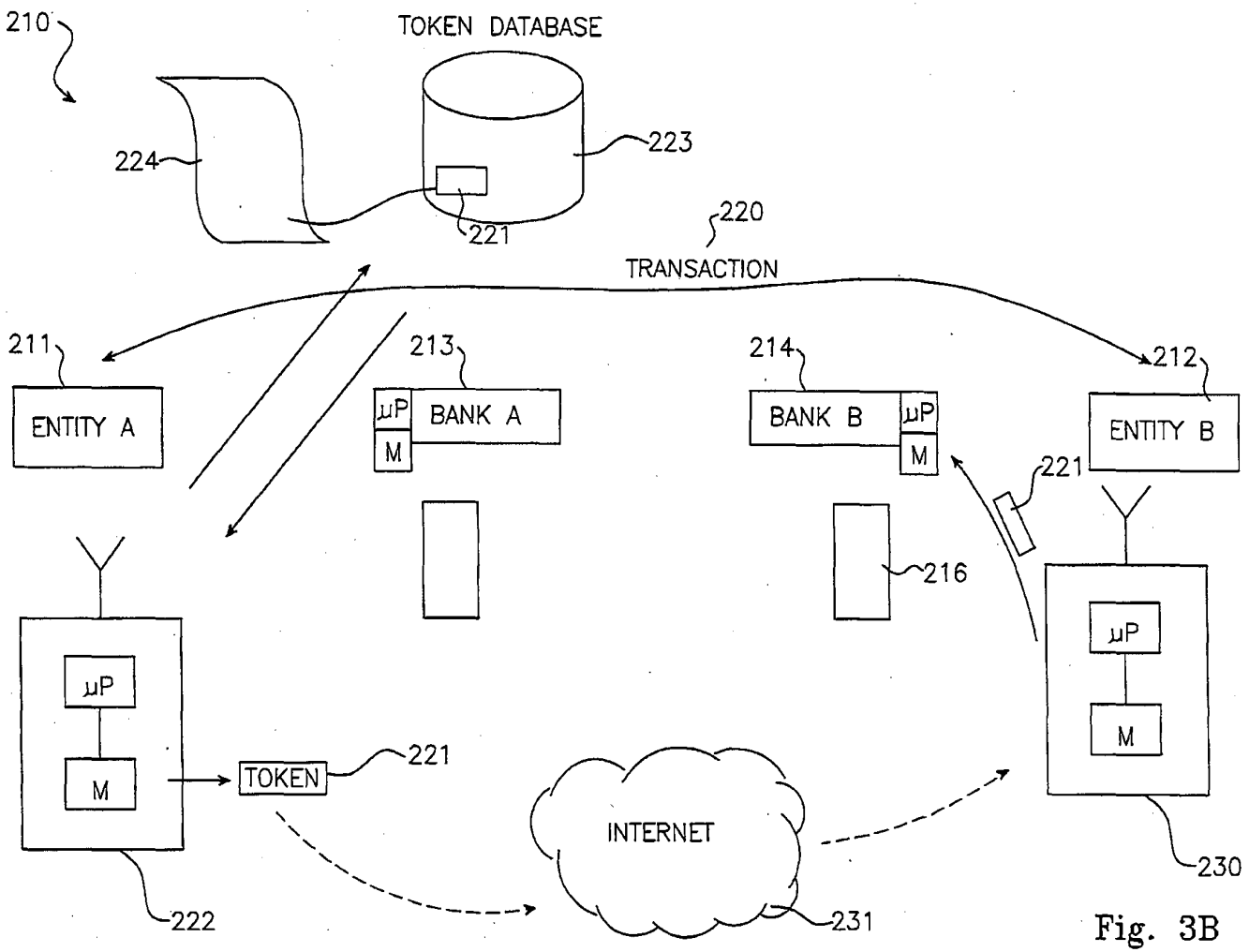

210
TOKEN DATABASE
224
223
221
220
TRANSACTION
211
213
214
212
ENTITY A
μP
BANK A
M
BANK B
μP
M
ENTITY B
221
216
μP
M
TOKEN
221
μP
M
INTERNET
230
222
231

Fig. 3B

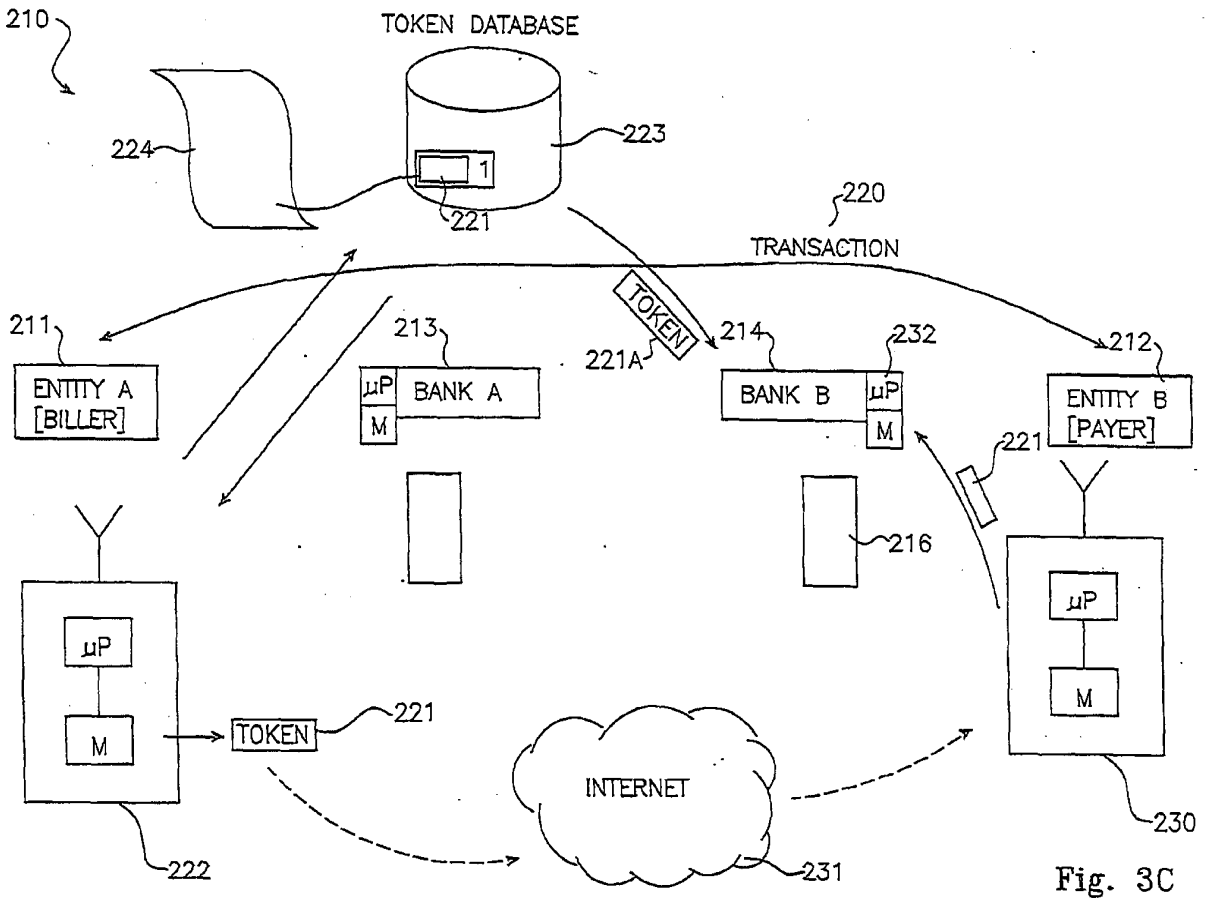
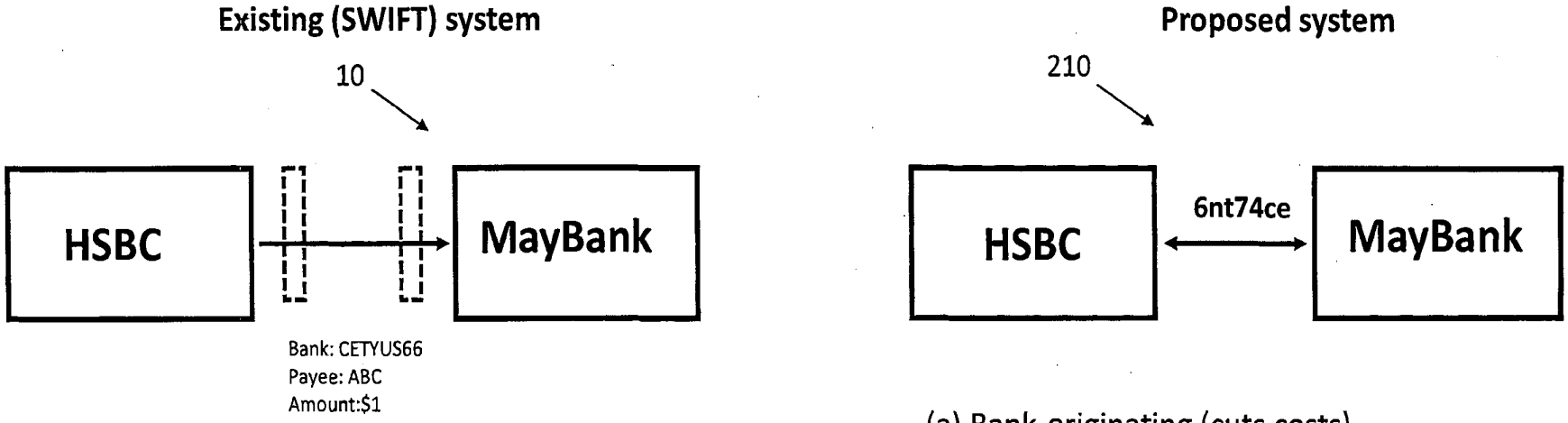

210
TOKEN DATABASE
224
223
1
221
220
TRANSACTION
TOKEN
221A
211
ENTITY A
[BILLER]
213
BANK A
μP
M
214
BANK B
232
212
ENTITY B
[PAYER]
216
TOKEN
221
INTERNET
222
231
230

Fig. 3C

8/16

Our token system gives power back to Banks to run their own shop; with their own, decentralized security management



(a) Depends on SWIFT infrastructure

(a) Bank-originating (cuts costs)

(b) Optional add-on: Data-enriched for PaaS for customers

(a) Depends on SWIFT infrastructure 2. SWIFT codes based on correspondent identifiers, so anyone can do it

Figure 4

We can curate our messaging system to accommodate Bank's risk appetite in relation to user data

Base Case

Fully anonymized data

Bank-powered
- Tokenization within bank
- User ID generation in banks

Benefit
- Processing cost
- Improved confidentiality of transaction data

Option A: XX

Text
- Text
  - Text

Option B: Data Rich

User ID shared with Sparro

Bank-powered
- Tokenization within bank
- User ID generation in banks

Benefit
- Processing cost
- Enriched Payments as a Service to Bank customers

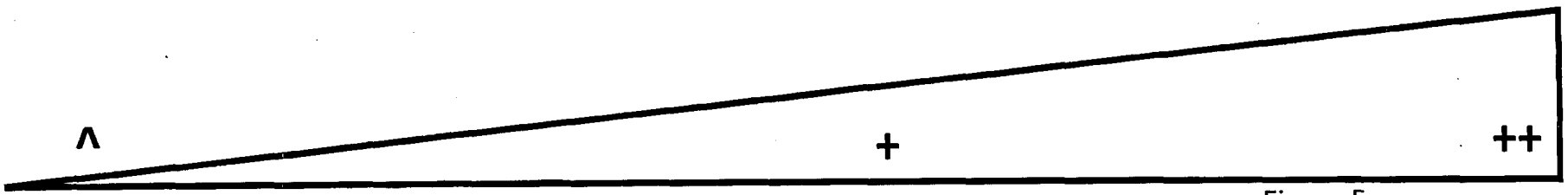


Figure 5

JPMC Ex. 1002
Page 446

SUMMARY: Benefits to Banks vis-a-vis SWIFT and Ripple

	Issue	SWIFT	Ripple	Proposed
470	Commercial	Bypass SWIFT	No competition, given infrastructure focus	1. Banks turn cost centre re SWIFT processing into profit pool 2. *Optional add-on*: new revenue from e.g.PaaS
471	Security	SWIFT-based	Block chain	1. Bank's private system
472	Technical	Committed infrastructure spend is slow and expensive	Private gateway establishment	Sparro (anonymized) messaging

Figure 6

JPMC Ex. 1002
Page 447

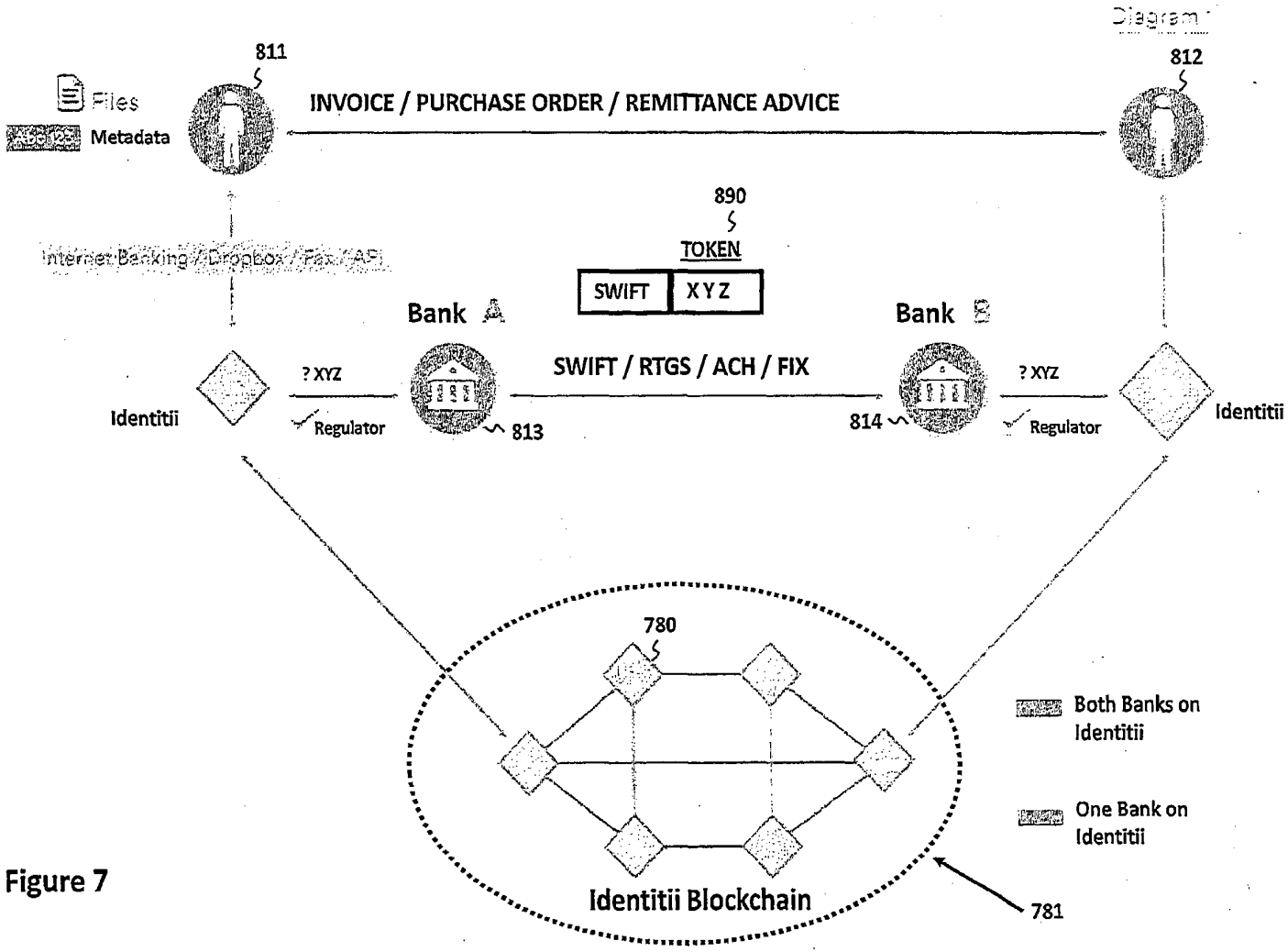
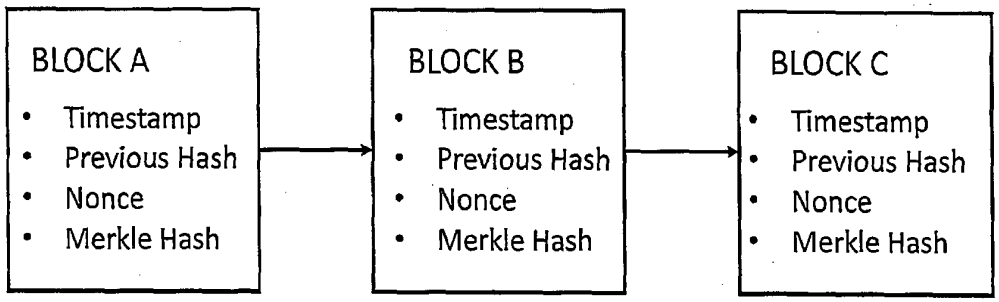


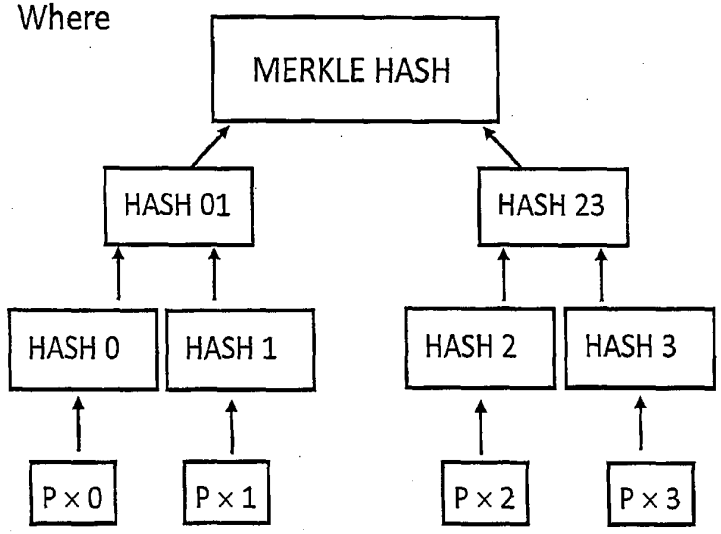
Figure 7

12/16

Figure 8 A



Where



JPMC Ex. 1002
Page 449

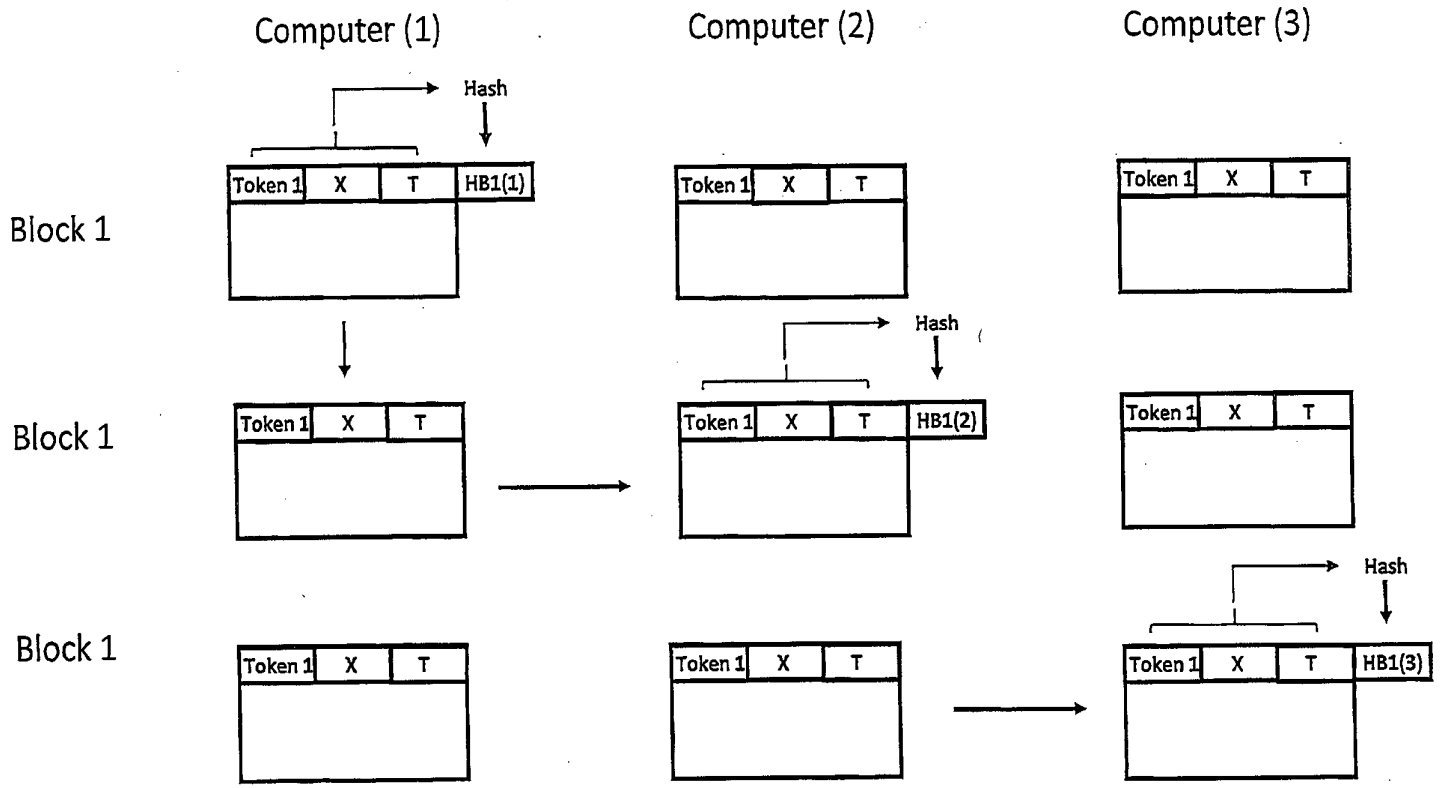

Computer (1)
Computer (2)
Computer (3)
Hash
Token 1
X
T
HB1(1)
Block 1
Block 1
HB1(2)
Block 1
HB1(3)

Figure 8B

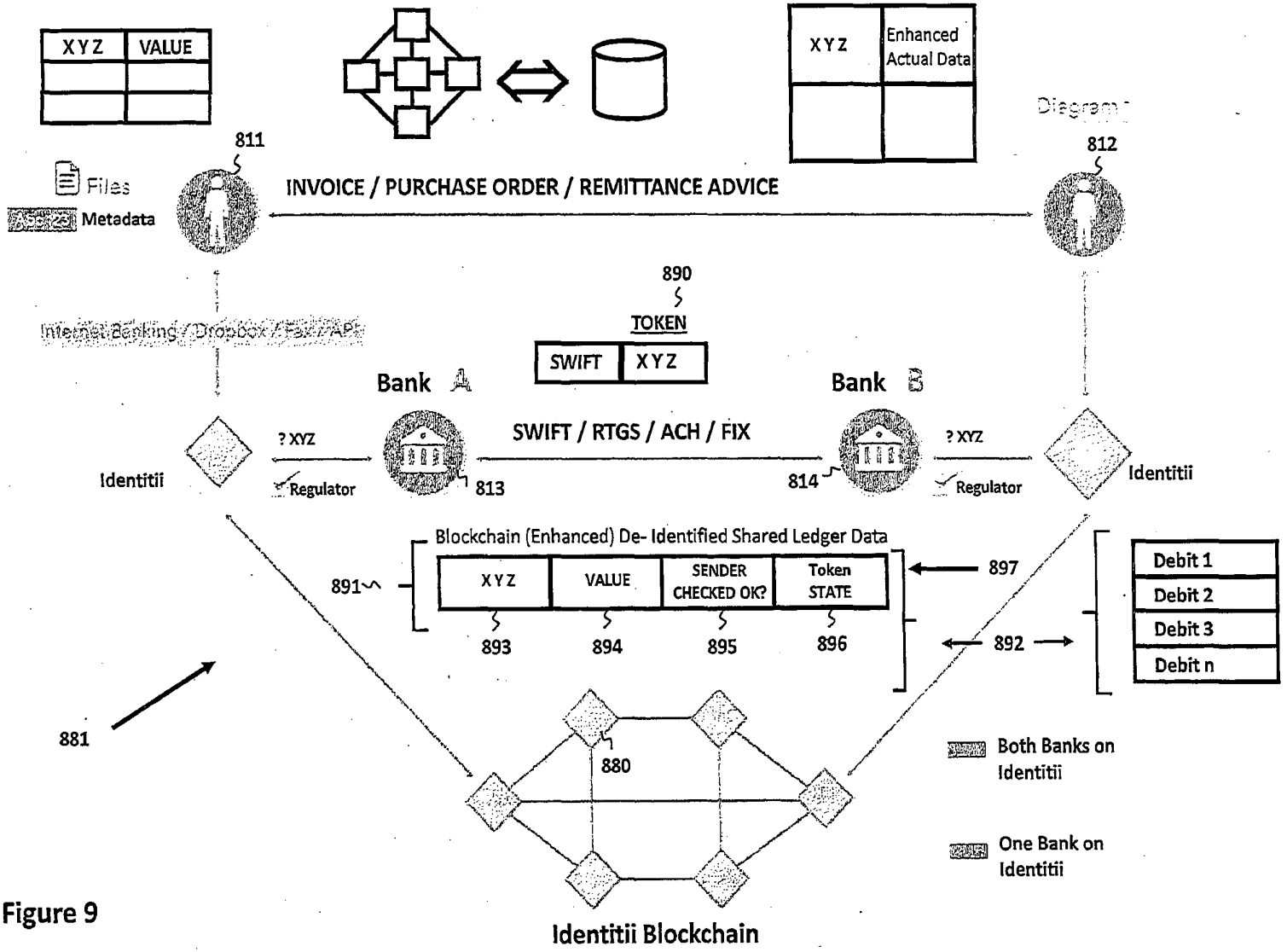
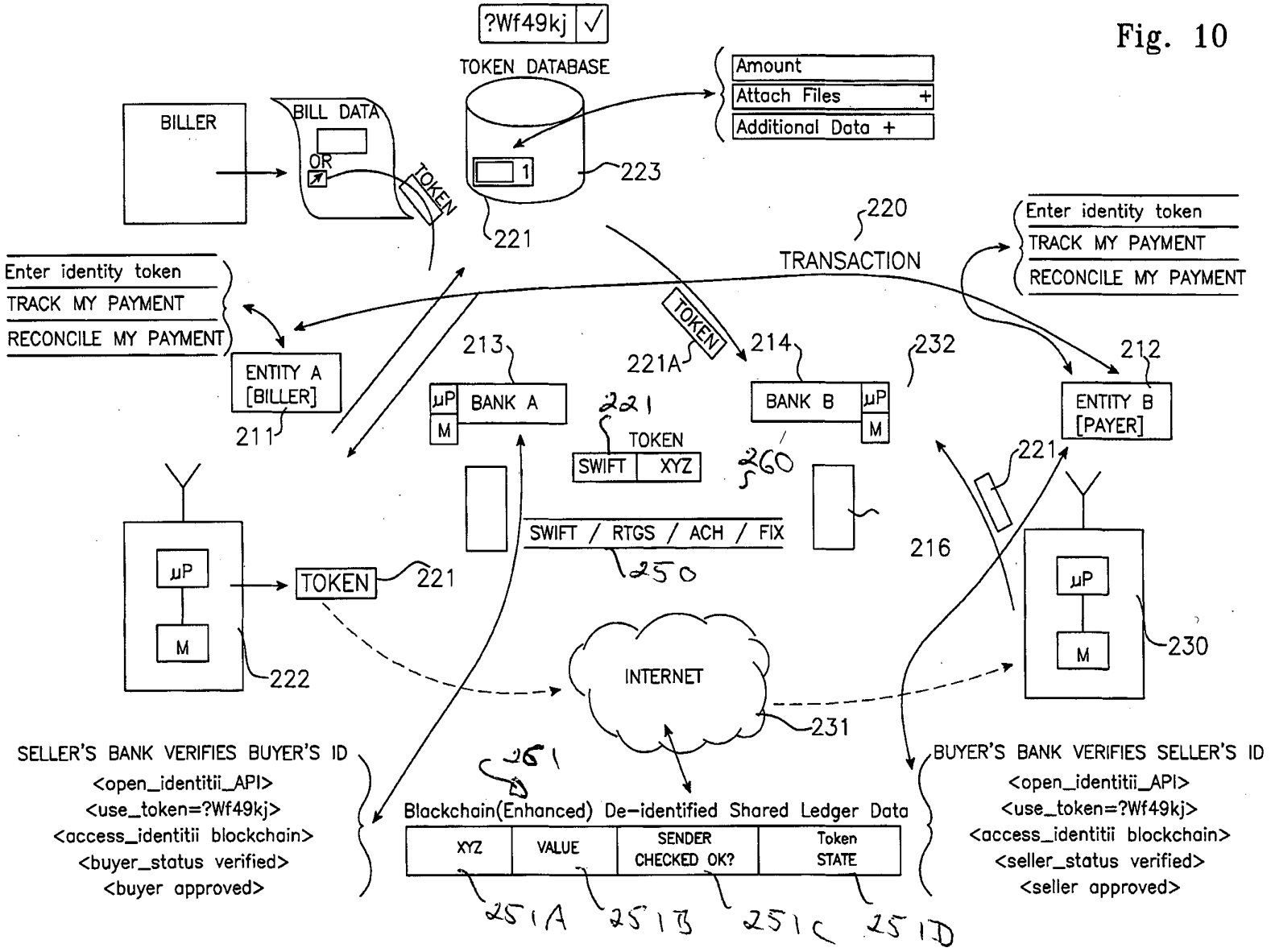


Figure 9

15/16

Fig. 10



JPMC Ex. 1002
Page 452

WIPO
WORLD
INTELLECTUAL PROPERTY
ORGANIZATION

DOCUMENT MADE AVAILABLE UNDER THE PATENT COOPERATION TREATY (PCT)

International application number:		**PCT/AU2016/000279**
International filing date:		**12 August 2016 (12.08.2016)**
Document type:		**Certified copy of priority document**
Document details:	Country/Office:	**AU**
	Number:	**2016901924**
	Filing date:	**20 May 2016 (20.05.2016)**
Date of receipt at the International Bureau:		**27 September 2016 (27.09.2016)**

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a),(b) or (b-*bis*)

34, chemin des Colombettes
1211 Geneva 20, Switzerland
www.wipo.int

Australian Government

PCT/AU2016/000279

Patent Office
Canberra

I, VIVIENNE IGLESIAS, DELEGATE OF THE COMMISSIONER, hereby certify that annexed is a true copy of the Provisional specification in connection with Application No. 2016900239 for a patent by SPARRO (AUSTRALIA) PTY LTD as filed on 27 January 2016.

WITNESS my hand this
THIRTEENTH day of September 2016

VIVIENNE IGLESIAS
DELEGATE OF THE COMMISSIONER

2016900239 27 Jan 2016

Payment Messaging System

TECHNICAL FIELD

[0001] The present invention relates to settlement systems and, more particularly although not exclusively, to a payment messaging system particularly, although not exclusively, suited to electronic transactions.

BACKGROUND

[0002] "Settlement" in the sense of settling amounts owing as between two parties, whether in a Fiat currency or in the newer forms of electronic currency (such as "Bitcoin") is a known concept which is central to the workings of most financial systems. In the case of electronic currency which requires settlement by exchange of data between institutions the current system is quite cumbersome and leads to many costs due in part to the necessity for often repeated data entry of significant amounts of data into systems run by the parties to any given transaction requiring settlement and also to the intermediaries that it almost every instance (barring a non-electronic cash transaction) form part of a chain of intermediaries that become involved in ultimately effecting settlement of any given transaction.

[0003] In particular implementations of settlement systems across the internet, a blockchain structure may be utilised where a blockchain is a distributed database that maintains a continuously growing list of data records that may be hardened against tampering and revision. The most widely known application of a blockchain is the public ledger of transactions for cryptocurrencies, such as Bitcoin referenced above.

[0004] Many settlement systems are characterised by effectively one-way transmission of data in any given data exchange transaction (for example systems based on Swift messaging). If it is subsequently discovered that there are deficiencies in the data thus transmitted there can then ensue time consuming checking and querying operations before settlement can be effected.

[0005] It is an object of the present invention to address or at least ameliorate some of the above disadvantages.

2016900239 27 Jan 2016

Notes

[0006] The term "comprising" (and grammatical variations thereof) is used in this specification in the inclusive sense of "having" or "including", and not in the exclusive sense of "consisting only of".

[0007] The above discussion of the prior art in the Background of the invention, is not an admission that any information discussed therein is citable prior art or part of the common general knowledge of persons skilled in the art in any country.

SUMMARY OF INVENTION

Definitions:

[0008] **token:** in this specification a "token" is a data record containing data required to settle a transaction for which the token has been generated; and wherein the data is rendered, formatted or passed through an algorithm in a predetermined manner. The process of rendering, formatting or passing through an algorithm in a predetermined manner is termed "tokenisation". The tokenisation process may involve operations such as encryption and de-identification of data.

[0009] **Transaction:** in this specification "transaction" refers to a trade between two parties, for example at least a first transacting entity and a second transacting entity and wherein the trade is expressed in a financial form (for example in a Fiat currency or an electronic currency-to be distinguished, for example, from a barter transaction) which will ultimately require exchange of currency to settle the transaction. In some instances the currency will be the same on both sides of the transaction. In other cases a conversion from one currency to another may be required.

[00010] Accordingly, in one broad form of the invention, there is provided a system for settling a transaction electronically; said system comprising:

at least a first transacting entity;

at least a second transacting entity;

at least a first intermediary entity;

at least a second intermediary entity;

2016900239 27 Jan 2016

in the case where the first transacting entity enters into a transaction with the second transacting entity generating a tokenised message at the time of the transaction containing data needed to settle the transaction;
initiating settlement of the transaction by transmission of the tokenised message to the at least first transacting entity.

[00011] In a further broad form of the invention there is provided a tokenised message construction system; said system comprising:
a server in communication with a database and which facilitates communications between a plurality of parties to a transaction;
each party having a digitised device with which to communicate with other ones of the parties and with the server;
each party capable of generating a tokenised message via a bidirectional communication with the server.

[00012] Preferably the tokenised message is generated with reference to a token database located at a remote location.

[00013] Preferably the tokenised message includes at least a first data element, a second data element and a third data element.

[00014] Preferably the first data element comprises identification data for a payor, the second data element comprises identification data for a payee (biller) and the third data element comprises identification currency, denomination and value data.

[00015] Preferably a further tokenised message is generated by either an intermediary entity or the token database.

[00016] Preferably a tokenised message is generated by a bi-directional communication process.

[00017] Preferably the bi-directional communication process is between the token database and an intermediary entity.

[00018] Preferably a step in producing a tokenised message involves de-identifying data.

2016900239 27 Jan 2016

[00019] Preferably a step in producing a tokenised message involves adding a data element to the message.

[00020] Preferably a step in producing a tokenised message involves removing a data element from the message.

[00021] Preferably a step in producing a tokenised message involves applying an algorithm to the data elements in the message.

[00022] Preferably the token database sequences the tokenised messages.

[00023] Preferably the token database sequences the tokenised messages and transmits the tokenised messages as payment data records to a blockchain settlement system.

[00024] Preferably the blockchain settlement system employs the Ripple protocol.

BRIEF DESCRIPTION OF DRAWINGS

[00025] Embodiments of the present invention will now be described with reference to the accompanying drawings wherein:

[00026] Figure 1A is a block diagram of the entities and intermediaries involved in a prior art electronic settlement system;

[00027] Figure 1B is a data and funds flow according to a prior art settlement system;

[00028] Figure 2A is a data and funds flow diagram according to an indicative embodiment of the present invention;

[00029] Figure 2C is a block diagram of the basic infrastructure and components suited for use with embodiments of the present invention and

[00030] Figure 3 A, B, C comprise block diagrams of the steps in a settlement transaction in accordance with a first preferred embodiment of the present invention

2016900239 27 Jan 2016

[00031] Figure 4 is a block diagram of salient characteristics of a messaging system 10 of the prior art as compared with the salient messaging characteristics of the system 210 enabled by the code of a second embodiment.

[00032] Figure 5 illustrates the options for data content to be included in tokens in accordance with embodiments of the invention as described above.

[00033] Figure 6 provides a comparison of characteristics of embodiments of the present invention as compared with the prior art Swift-based messaging system.

[00034] Figure 7 is a block diagram in accordance with a further preferred embodiment of the present invention.

[00035] Figure 8 is a block diagram of an implementation of a blockchain arrangement suitable for use with the system of earlier embodiments.

DESCRIPTION OF EMBODIMENTS

[00036] With reference to Figure 1A there is illustrated in block form the basic components of a prior art settlement system. In many transactions there will be an at least first transacting entity 11 which enters into a transaction with an at least second transacting entity 12. The transaction may be as simple as the agreement by the first transacting entity 11 to sell a particular item or service to the second transacting entity 12. Typically the transaction will require settlement for an agreed amount expressed in a Fiat or other currency. In the vast majority of cases the at least first transacting entity 11 will be associated with an at least first intermediary entity 13, in this instance in the form of a bank A and similarly the second transacting entity 12 will be associated with an at least second intermediary entity 14 in this instance in the form of bank B. The first transacting entity 11 will have a first bank account 15 at the first intermediary entity 13 whilst second transacting entity 12 will have a second bank account 16 at second intermediary entity 14. Settlement of any given transaction requires instruction given by first transacting entity 11 to its first intermediary entity 13 to pay an agreed amount from the first bank account 15 to the bank account comprising second bank account 16 of second intermediary entity 14 of second transacting entity 12. For these instructions to be carried out metadata in the form of payment metadata 17 must be assembled at the first intermediary entity 13 sufficient and exhaustive to communicate to the second intermediary entity 14 such that the agreed settlement amount is transmitted from bank A to bank B and more particularly to the specific accounts of the respective first transacting entity 11 and second transacting entity 12.

2016900239 27 Jan 2016

[00037] A similar transaction may be applied in reverse where the second transacting entity sells a good or service to first transacting entity 11. In such an instance the respective intermediaries, once having received the respective payment metadata 17 and exchanged that metadata 17 may elect to simply pay the difference 18 electronically as between the intermediaries to effect the multiple transactions. In some instances, particularly where the transaction is cross-border-for example the first intermediary entity 13 is in a first country whilst the second intermediary entity 14 is in a second country the metadata 17 may include what is known as a Swift code which is a substantially unique identifier for each intermediary entity involved in the transaction. However, for any given transaction, far more data than merely a unique identifier for each intermediary entity involved in a transaction is required in order for the appropriate settlement amounts to ultimately be recorded in the correct accounts and settle the transaction for the agreed amounts.

[00038] Figure 1B is a data and funds flow diagram of data and funds flow according to a prior art settlement system at the granular level. In this instance, with reference to figure 1B like components are numbered as for figure 1A a given transaction requiring settlement can be embodied as a bill 90 which will include payment data 91 and may include bank facilitation payment data 92 comprising, in this instance, a biller code and a transaction code. Banks which are party to this bank facilitation payment system permit data entry by entity B (or payer B) 12 into a database of bank B 14 by means of a bank application or web interface 14 B. Bank B may then add additional data to form metadata 17 which is sent to a third-party server 93 which utilises metadata 17 to trigger pay (settlement) of bill 90 from payer B bank 14 to biller A bank 13.

Generalised Embodiment:

[00039] With reference to Figure 2C there is illustrated a block diagram of the basic infrastructure and components suited for use with embodiments of the present invention. In this instance like components are numbered as for figure 1 except in the 100 series. So, for example, first transacting entity 11 becomes first transacting entity 111 in this embodiment with reference to figure 2C.

[00040] In this instance a settlement system 110 according to a generalised embodiment includes at least first transacting entity 111 which enters into a transaction with at least a second transacting entity 112. As previously these entities are associated with a respective first

2016900239 27 Jan 2016

intermediary entity 113 and a second intermediary entity 114 in the form of bank A and bank B. Each of the first transacting entity 111 and a second transacting entity 112 has a respective account 115, 116 at their respective intermediary entities as illustrated in figure 2C

[00041] In this instance, in the event that first transacting entity 111 enters into a transaction with second transacting entity 112 then, at the time of entry into the transaction 120, a token 121 is generated. In this instance the token 121 is generated by at least first digital device 122 communicating with a token database 123. The token database 123 generates a token comprising a data file 124 containing all data that will ultimately be required to settle the transaction 120 including any necessary identifying information for the transacting entity is, their accounts and the intermediary entities. Settlement is effected by communication of the token 121 to bank A and then to bank B together with the appropriate flow of funds.

[00042] With reference to figure 2A at the granular level a bill 190 from a biller 111 directed to a payer 112 contains bill data 191 and also token data of a token 121 residing within a code symbol 194 (in this instance a QR code). The token data includes pointer data pointing to data 195 on token database 123. The data 195 combined with bank ID data 114 permits the creation by token database 123 of a full payment record 196 which can be utilised to cause settlement of the bill 190 as against payer 112 via, in this instance, their respective banks 114, 113.

[00043] With reference to figure 2B the payment data record 196 is utilised has fed into a settlement network such as, for example a network 197 operating under the Ripple protocol thereby permitting substantially real-time settlement across multiple institutions and banks.

First Embodiment:

[00044] With reference to Figures 3 there is illustrated in block diagram form a first preferred embodiment of the present invention by way of a non-limiting example of a transaction. In this embodiment like components are numbered as for the previous embodiments except in the 200 series. So, for example, token 121 becomes token 221.

[00045] With reference to figure 3A the transaction system 210 is activated, as for the previous embodiment, when a transaction 220 is entered into between at least first transacting entity 211 and at least a second transacting entity 212 each dealing, for the purposes of this transaction, through respective intermediary entities 213, 214.

2016900239 27 Jan 2016

[00046] At the time of and as part of entry into the transaction 220 the first transacting entity 211 accesses token database 223 via digital device 222 executing via a web browser interface or via execution of an application running on a portable digital devices such as a mobile telephone or in a further alternative as a point-of-sale terminal in order to arrange for the database 223 to generate a token 221. In this instance the token 221 will include better data 224 including the recipient named, BIC, IBAN, destination country, mobile number, currency, business type, communication, payment amount. In this instance the token 221 including the metadata 224 is stored in the token database 223. In addition the first transacting entity 211 communicates the token 221 to a digital device 230 associated with second transacting entity 212. In this instance the communication is by way of initial transmission of the token 221 to digital device 222 which then on transmits the token via Internet 231 to digital device 230.

[00047] With reference to figure 3B, when ready to settle the transaction 220 the second transacting entity 212 "logs in" to a portal associated with second intermediary entity 214 and communicates the token 221. In this instance have the login can be executed via a web browser associated with digital device 230 which communicates via Internet 231 the token 221 to a digital processing system 232 (including at least a processor and a memory) associated with second intermediary entity 214. Substantially at the same time as part of seeking to settle the transaction 220:

[00048] Notification: token database 223 notifies second intermediary entity 214 to contact the token database 223 from which it receives a further token 221A.

[00049] Verification: token database 223 communicates with the processing system 232 of second intermediary entity 214 to verify that sufficient funds are located in account 216 as indicated in the meta data 224 to settle the transaction.

[00050] Committing payer funds: payers bank debits payers account: payers bank sends notice to payer bank gateway: payers bank gateway calls token database 223 to get approved token:

[00051] Settlement: gateway of payers bank sends by way of non limiting example XRP (the native currency of the Ripple protocol) to billers bank gateway: payers bank gateway notifies token database 223 of receipt:

[00052] Clearing: payer's bank Nostro account is debited subject to bank institution rules.

2016900239 27 Jan 2016

[00053] Embodiments of the invention can be implemented utilising the "Ripple" the framework, protocol and gateway-or more generally any blockchain based framework. In a particular form the final settlement process can be enabled through a Ripple frame work thereby to facilitate substantially real-time settlement across multiple institutions and multiple banks.

Second Embodiment:

[00054] Examples of tokenised messages and their generation and transmission are illustrated in pseudocode below. Reference to "sparro" is a reference to an instance of a token database123.

[00055] The previous, meta-data mode is first. It switches to minimal half way through

```
--
Bank:HSBC >> createUserCode >> Sparro:Sparro
  {"id":"User:ABC Paper","name":"ABC Paper"}
(Creating Sparro User Code - Meta-data given can be used by other banks for compliance and
for confirming payee with customers.)

--
Bank:MayBank >> createUserCode >> Sparro:Sparro
  {"id":"User:XYZ Printing","name":"XYZ Printing"}
(Creating Sparro User Code - Meta-data given can be used by other banks for compliance and
for confirming payee with customers.)
--
Sparro:Sparro >> createUserCode-reply >> Bank:HSBC
  {"id":"User:ABC Paper","name":"ABC Paper","code":"65q3gdd"}
--
Sparro:Sparro >> createUserCode-reply >> Bank:MayBank
  {"id":"User:XYZ Printing","name":"XYZ Printing","code":"70wqgx6"}

--
User:ABC Paper >> createInvoice >> Bank:HSBC
  {"amount":{"amount":1000,"currency":"gbp"}}

--
```

2016900239 27 Jan 2016

Bank:HSBC >> createInvoiceCode >> Sparro:Sparro

{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd"}

(Creating Invoice Code - An invoice code is created by Sparro and connected to the bank.)

-

Sparro:Sparro >> createInvoiceCode-reply >> Bank:HSBC

{"code":"6tq6wcbad"}

--

Bank:HSBC >> createInvoice-reply >> User:ABC Paper

{"invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

Abc invoice { amount: { amount: 1000, currency: 'gbp' },
payee: '65q3gdd',
code: '6tq6wcbad' }

--

User:ABC Paper >> invoice >> User:XYZ Printing

{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}

-

User:XYZ Printing >> payInvoice >> Bank:MayBank

{"invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300}}

--

Bank:MayBank >> sendMoney >> BankGateway:MayBank

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300}}

--

BankGateway:MayBank >> getInvoice >> Sparro:Sparro

"6tq6wcbad"

(Sending Payment to Invoice - The payment is sent to the bank that created the invoice.)

--

Sparro:Sparro >> getInvoice-reply >> BankGateway:MayBank

{"bank":"Bank:HSBC","invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

2016900239 27 Jan 2016

--

BankGateway:MayBank >> transfer >> BankGateway:HSBC

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":"ripple-1"}

--

BankGateway:HSBC >> incomingTransfer >> Bank:HSBC

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":"ripple-1"}

--

BankGateway:HSBC >> transfer-reply >> BankGateway:MayBank

{"success":true,"owed":{"GBP":300}}

--

Bank:HSBC >> getInvoice >> Sparro:Sparro

"6tq6wcbad"

--

BankGateway:MayBank >> sendMoney-reply >> Bank:MayBank

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":"ripple-1"}

--

Sparro:Sparro >> getInvoice-reply >> Bank:HSBC

{"bank":"Bank:HSBC","invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

--

Bank:MayBank >> payInvoice-reply >> User:XYZ Printing

2016900239 27 Jan 2016

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":
"ripple-1"}

XYZ part-paid invoice {
"payer": "70wqgx6",
"invoice": "6tq6wcbad",
"amount": {
"currency": "GBP",
"amount": 300
},
"id": "ripple-1"
}

--

Bank:HSBC >> incomingTransfer >> User:ABC Paper

{"invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcb
ad"},"transfer":{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amo
unt":300},"id":"ripple-1"}}

-

User:XYZ Printing >> payInvoice >> Bank:MayBank

{"invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700}}

--

Bank:MayBank >> sendMoney >> BankGateway:MayBank

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700}}

--

BankGateway:MayBank >> getInvoice >> Sparro:Sparro

"6tq6wcbad"

(Sending Payment to Invoice - The payment is sent to the bank that created the invoice.)

2016900239 27 Jan 2016

--

Sparro:Sparro >> getInvoice-reply >> BankGateway:MayBank

{"bank":"Bank:HSBC","invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

--

BankGateway:MayBank >> transfer >> BankGateway:HSBC

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700},"id":"ripple-2"}

--

BankGateway:HSBC >> incomingTransfer >> Bank:HSBC

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700},"id":"ripple-2"}

--

BankGateway:HSBC >> transfer-reply >> BankGateway:MayBank

{"success":true,"owed":{"GBP":1000}}

--

Bank:HSBC >> getInvoice >> Sparro:Sparro

"6tq6wcbad"

-

BankGateway:MayBank >> sendMoney-reply >> Bank:MayBank

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700},"id":"ripple-2"}

--

Sparro:Sparro >> getInvoice-reply >> Bank:HSBC

2016900239 27 Jan 2016

{"bank":"Bank:HSBC","invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

--

Bank:MayBank >> payInvoice-reply >> User:XYZ Printing

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700},"id":"ripple-2"}

XYZ finished paying invoice {

"payer": "70wqgx6",
"invoice": "6tq6wcbad",
"amount": {
"currency": "GBP",
"amount": 700
},
"id": "ripple-2"

}

--- SWITCHING TO MODE: minimal ---

--

Bank:HSBC >> incomingTransfer >> User:ABC Paper

{"invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"},"transfer":{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700},"id":"ripple-2"}}

--Bank:HSBC >> createUserCode >> Sparro:Sparro

undefined

(Creating Sparro User Code - No meta-data is required.)

2016900239 27 Jan 2016

--

Bank:MayBank >> createUserCode >> Sparro:Sparro

undefined

(Creating Sparro User Code - No meta-data is required.)

--

Sparro:Sparro >> createUserCode-reply >> Bank:HSBC

{"code":"dnt7gec"}

--

Sparro:Sparro >> createUserCode-reply >> Bank:MayBank

{"code":"6wwpwuc"}

--

User:ABC Paper >> createInvoice >> Bank:HSBC

{"amount":{"amount":2000,"currency":"gbp"}}

--

Bank:HSBC >> createInvoiceCode >> Sparro:Sparro

null

(Creating Invoice Code - An invoice code is created by Sparro and connected to the bank. No invoice details are required.)

--

Sparro:Sparro >> createInvoiceCode-reply >> Bank:HSBC

{"code":"erwkax1md"}

--Bank:HSBC >> createInvoice-reply >> User:ABC Paper

{"invoice":{"amount":{"amount":2000,"currency":"gbp"},"code":"erwkax1md","payee":"User: ABC Paper","transfers":[]}}

2016900239 27 Jan 2016

Abc invoice { amount: { amount: 2000, currency: 'gbp' },
code: 'erwkax1md',
payee: 'User:ABC Paper',
transfers: [] }

--

User:ABC Paper >> invoice >> User:XYZ Printing

{"amount":{"amount":2000,"currency":"gbp"},"code":"erwkax1md","payee":"User:ABC Paper","transfers":[]}

--

User:XYZ Printing >> payInvoice >> Bank:MayBank

{"invoice":"erwkax1md","amount":{"currency":"GBP","amount":600}}

--

Bank:MayBank >> sendMoney >> BankGateway:MayBank

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600}}

--

BankGateway:MayBank >> getInvoice >> Sparro:Sparro

"erwkax1md"

(Sending Payment to Invoice - The payment is sent to the bank that created the invoice.)

--

Sparro:Sparro >> getInvoice-reply >> BankGateway:MayBank

{"bank":"Bank:HSBC"}

--

BankGateway:MayBank >> transfer >> BankGateway:HSBC

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}

--

2016900239 27 Jan 2016

BankGateway:HSBC >> incomingTransfer >> Bank:HSBC

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}

--

BankGateway:HSBC >> transfer-reply >> BankGateway:MayBank

{"success":true,"owed":{"GBP":600}}

--

Bank:HSBC >> incomingTransfer >> User:ABC Paper

{"invoice":{"amount":{"amount":2000,"currency":"gbp"},"code":"erwkax1md","payee":"User:ABC Paper","transfers":[{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}]},"transfer":{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}}

--

BankGateway:MayBank >> sendMoney-reply >> Bank:MayBank

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}

--

Bank:MayBank >> payInvoice-reply >> User:XYZ Printing

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}

XYZ part-paid invoice {

"payer": "6wwpwuc",
"invoice": "erwkax1md",
"amount": {

2016900239 27 Jan 2016

"currency": "GBP",
"amount": 600
},
"id": "ripple-3"
}

--

User:XYZ Printing >> payInvoice >> Bank:MayBank

{"invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400}}

--

Bank:MayBank >> sendMoney >> BankGateway:MayBank

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400}}

--

BankGateway:MayBank >> getInvoice >> Sparro:Sparro

"erwkax1md"

(Sending Payment to Invoice - The payment is sent to the bank that created the invoice.)

--

Sparro:Sparro >> getInvoice-reply >> BankGateway:MayBank

{"bank":"Bank:HSBC"}

-

BankGateway:MayBank >> transfer >> BankGateway:HSBC

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}

--

BankGateway:HSBC >> incomingTransfer >> Bank:HSBC

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}

2016900239 27 Jan 2016

BankGateway:HSBC >> transfer-reply >> BankGateway:MayBank
{"success":true,"owed":{"GBP":2000}}

--

Bank:HSBC >> incomingTransfer >> User:ABC Paper

{"invoice":{"amount":{"amount":2000,"currency":"gbp"},"code":"erwkax1md","payee":"User:ABC
Paper","transfers":[{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"},{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}]},"transfer":{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}}

--

BankGateway:MayBank >> sendMoney-reply >> Bank:MayBank

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}

--

Bank:MayBank >> payInvoice-reply >> User:XYZ Printing

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}

XYZ finished paying invoice {
"payer": "6wwpwuc",
"invoice": "erwkax1md",
"amount": {

2016900239 27 Jan 2016

"currency": "GBP",
"amount": 1400
},
"id": "ripple-4"
}

features of this embodiment include the enablement of a private, invitation only, network for banking institutions which, in a particular form, can facilitate cross-border payments thereby to enable substantially real-time payments at reduced processing cost.

[00056] With reference to figure 4 there is shown a block diagram of salient characteristics of a messaging system 10 of the prior art as compared with the salient messaging characteristics of the system 210 enabled by the code listed above and more broadly described with reference to the earlier embodiments.

[00057] Figure 5 illustrates the options for data content to be included in tokens in accordance with embodiments of the invention as described above.

[00058] Figure 6 provides a comparison of characteristics of embodiments of the present invention as compared with the prior art Swift-based messaging system at a commercial layer 470, a security layer 471 and a technical layer 472.

Further Embodiment

[00059] Figure 7 is a block diagram of a further embodiment. In this instance a distributed ledger 781 operating on blockchain principles provides for transmission of the tokenised message as for previous embodiments.

[00060] In this instance it will be observed that the tokenised transmission distributed ledger 781 operates in parallel with conventional transmission between institution A and institution B.

[00061] Conventional transmission includes transmission of conventional messages utilising the SWIFT protocol. It is also to be noted that institution A and institution B may be subsidiaries of the same institution or may otherwise be closely related. In the alternative they may be completely independent institutions.

2016900239 27 Jan 2016

[00062] The tokenised message as described in previous embodiments may include information as typically transmitted by the SWIFT or other current acknowledged data transmission systems for transmission of financial information for the purpose of transfer of funds between parties.

[00063] The tokenised message may transmit data which includes some of the data normally included in the conventional message. In alternative forms it may include additional data. In yet alternative forms it may include data not transferred at all in the data normally included in the conventional message.

[00064] The aim, ultimately, is to improve the reliability of the transaction as between the first transacting entity and the second transacting entity and, in some forms, to provide an enhanced capability.

[00065] In the arrangement of figure 7 the data comprising the tokenised message is transmitted via nodes 780 within a blockchain 781.

[00066] In summary, Bank A and Bank B might be branches of the same bank, say HSBC HK and HSBC China (which today use SWIFT for intrabank transfers). So this system could be used within 1 financial institution.

[00067] In one form the purpose of storing the token only in the blockchain is really to both de-identify the information in the blockchain (which is critical for banks), and enable use of existing (SWIFT / ACH / RTGS) or new messaging systems to send the payment instruction in tokenised format. Banks today have significant investment in existing conventional messaging systems and a complete abandonment of these messaging systems would not be feasible. However settlement is still a manual process so linking the conventional messaging system to the 'blockchain' settlement system (via the token) is an important feature of this embodiment. So, in diagram 7 we include a SWIFT/ACH/RTGS connection between the two Financial Institutions (FIs) (or branches) for communication of the token, and the blockchain ledger is common. The data that is required to settle the payment can be provided by the FI's customer or by the FI themselves (say from a core banking system or similar).

[00068] Fig 8 illustrates in block diagram form key components of an implementation of a blockchain structure which may be utilised to implement the system of figure 7.

2016900239 27 Jan 2016

[00069] Each block includes verified transactions and the blockchain maintains a ledger all prior transactions. The blockchain is duplicated by all the computers on a network.

[00070] The first block in the chain is known as the Genesis block and new blocks can be added in linear and chronological order. From any given block in the chain the information of this genesis block and all blocks that led back to this one can be retrieved. A blockchain is essentially numerous blocks connected through hash chaining where each block is comprised of the following (see figure 8);

- Timestamp: provides proof that the data in a block existed at a particular time
- Previous Hash: Essentially a pointer to the previous block
- Merkle Hash: Summary of all executed transactions
- Nonce: Individual blocks identity and is an arbitrary number which can only be used once

[00071] The blockchain is managed by a network of distributed nodes where each node contains a copy of the entire blockchain. Each node in the network can add blocks to the chain, where every node is adding blocks at the same point in the chain at the same time. The more nodes that comprise the network the harder it is to disrupt the storage of the blockchain. Unlike centralised systems which rely on a single authority, there is no single point of failure in these distributed nodes network. If you change the content of a block you change its Hash.

[00072] Blockchains can be based on/ operate in association with any one of a number of protocols – for example Ripple or Stellar.

[00073] The above describes only some embodiments of the present invention and modifications, obvious to those skilled in the art, can be made thereto without departing from the scope of the present invention.

2016900239 27 Jan 2016

CLAIMS

1. A system for settling a transaction electronically; said system comprising:
   a) at least a first transacting entity;
   b) at least a second transacting entity;
   c) at least a first intermediary entity;
   d) at least a second intermediary entity;
   e) in the case where the first transacting entity enters into a transaction with the second transacting entity generating a tokenised message at the time of the transaction containing data needed to settle the transaction;
   f) initiating settlement of the transaction by transmission of the tokenised message between at least two of the entities..
2. The system of claim 1 wherein the tokenised message is generated with reference to a token database located at a remote location.
3. The system of claim 2 wherein the tokenised message includes at least a first data element, a second data element and a third data element.
4. The system of claim 3 wherein the first data element comprises identification data for a payor, the second data element comprises identification data for a payee (biller) and the third data element comprises identification currency, denomination and value data.
5. The system of claim 1 or claim 2 wherein a further tokenised message is generated by either an intermediary entity or the token database.
6. The system of any previous claim wherein a tokenised message is generated by a bi-directional communication process.
7. The system of claim 6 wherein the bi-directional communication process is between the token database and an intermediary entity.
8. The system of any previous claim wherein a step in producing a tokenised message involves de-identifying data.
9. The system of any previous claim wherein a step in producing a tokenised message involves adding a data element to the message.
10. The system of any previous claim wherein a step in producing a tokenised message involves removing a data element from the message.
11. The system of any previous claim wherein a step in producing a tokenised message involves applying an algorithm to the data elements in the message.

2016900239 27 Jan 2016

12. The system of any previous claim wherein the token database sequences the tokenised messages.
13. The system of any previous claim wherein the token database sequences the tokenised messages and transmits the tokenised messages as payment data records to a blockchain settlement system.
14. The system of claim 13 wherein the blockchain settlement system employs the Ripple protocol.
15. A tokenised message construction system; said system comprising:
    a) a server in communication with a database and which facilitates communications between a plurality of parties to a transaction;
    b) each party having a digitised device with which to communicate with other ones of the parties and with the server;
    c) each party capable of generating a tokenised message via a bidirectional communication with the server.
16. The system of claim 15 wherein the tokenised message is generated with reference to a token database located at a remote location.
17. The system of claim 16 wherein the tokenised message includes at least a first data element, a second data element and a third data element.
18. The system of claim 17 wherein the first data element comprises identification data for a payor, the second data element comprises identification data for a payee (biller) and the third data element comprises identification currency, denomination and value data.
19. The system of claim 15 or claim 16 wherein a further tokenised message is generated by either an intermediary entity or the token database.
20. The system of any one of claims 15 to 19 wherein a tokenised message is generated by a bi-directional communication process.
21. The system of claim 20 wherein the bi-directional communication process is between the token database and an intermediary entity.
22. The system of any one of claims 15 to 21 wherein a step in producing a tokenised message involves de-identifying data.
23. The system of any one of claims 15 to 22 wherein a step in producing a tokenised message involves adding a data element to the message.
24. The system of any one of claims 15 to 23 wherein a step in producing a tokenised message involves removing a data element from the message.

2016900239 27 Jan 2016

25. The system of any one of claims 15 to 24 wherein a step in producing a tokenised message involves applying an algorithm to the data elements in the message.
26. The system of any one of claims 15 to 25 wherein the token database sequences the tokenised messages.
27. The system of any one of claims 15 to 26 wherein the token database sequences the tokenised messages and transmits the tokenised messages as payment data records to a blockchain settlement system.
28. The system of claim 27 wherein the blockchain settlement system employs the Ripple protocol.
29. The system of any previous claim wherein a second message is transmitted between the intermediaries.
30. The system of claim 29 wherein the second message is tokenised.
31. The system of claim 29 or 30 wherein the second message contains conventional data.
32. The system of claim 29 or 30 or 31 wherein the second message is transmitted by means of a blockchain system.
33. The system of claim 29 or 30 or 31 wherein the second message includes information equivalent to that transmitted by the SWIFT system.
34. The system of claim 29 or 30 or 31 wherein the tokenised message includes additional information beyond that transmitted by the SWIFT system.
35. The system of claim 35 wherein the tokenised message includes information which verifies the security status of at least one party to the transaction.
36. The system of claim 35 wherein the second tokenised message includes information which verifies the security status of both parties to the transaction.

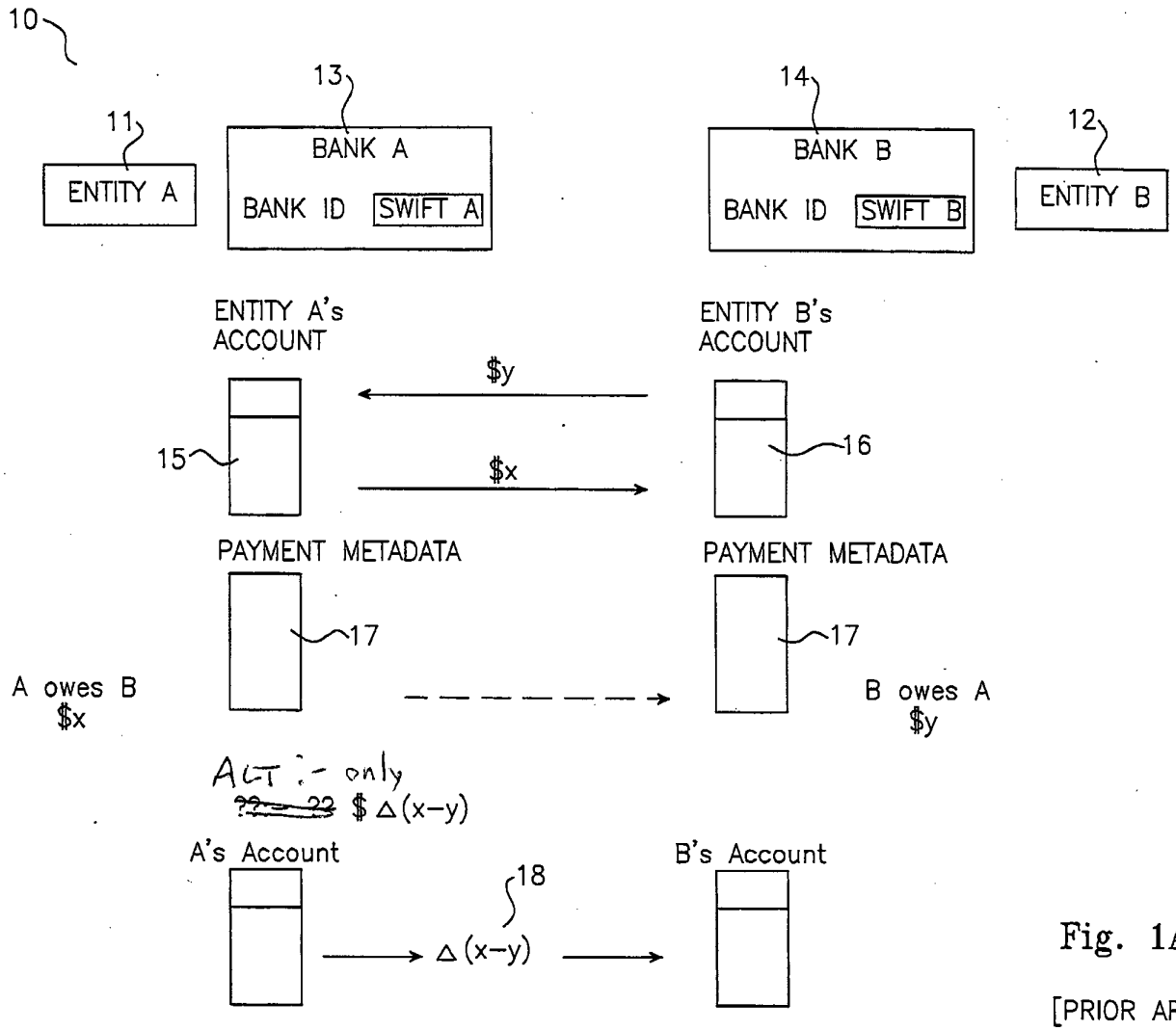


Fig. 1A

[PRIOR ART]

JPMC Ex. 1002
Page 480

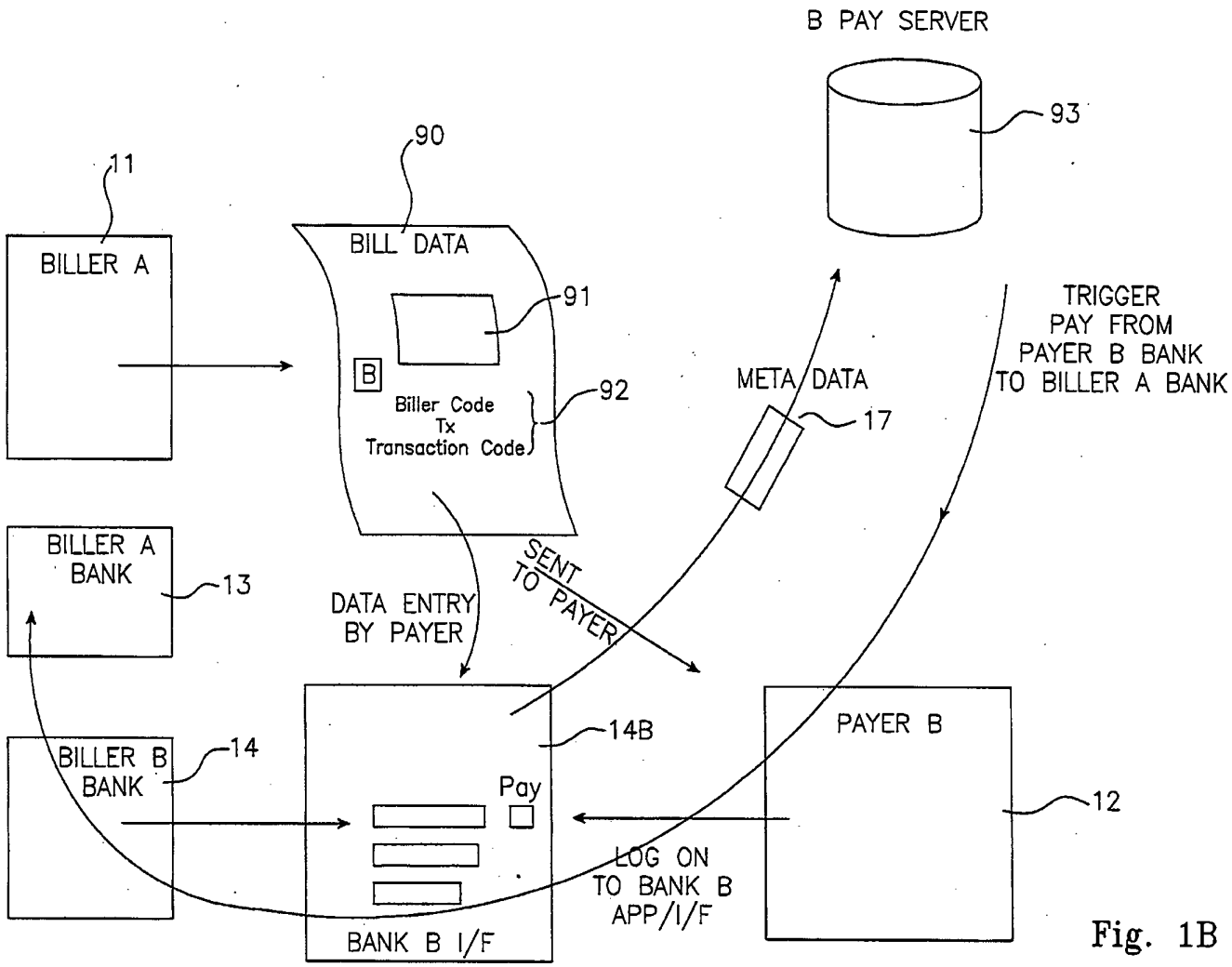

B PAY SERVER
93
90
11
BILLER A
BILL DATA
91
B
92
Biller Code
Tx
Transaction Code
META DATA
17
TRIGGER
PAY FROM
PAYER B BANK
TO BILLER A BANK
BILLER A
BANK
13
DATA ENTRY
BY PAYER
SENT
TO PAYER
14B
PAYER B
BILLER B
BANK
14
Pay
12
LOG ON
TO BANK B
APP/I/F
BANK B I/F

Fig. 1B

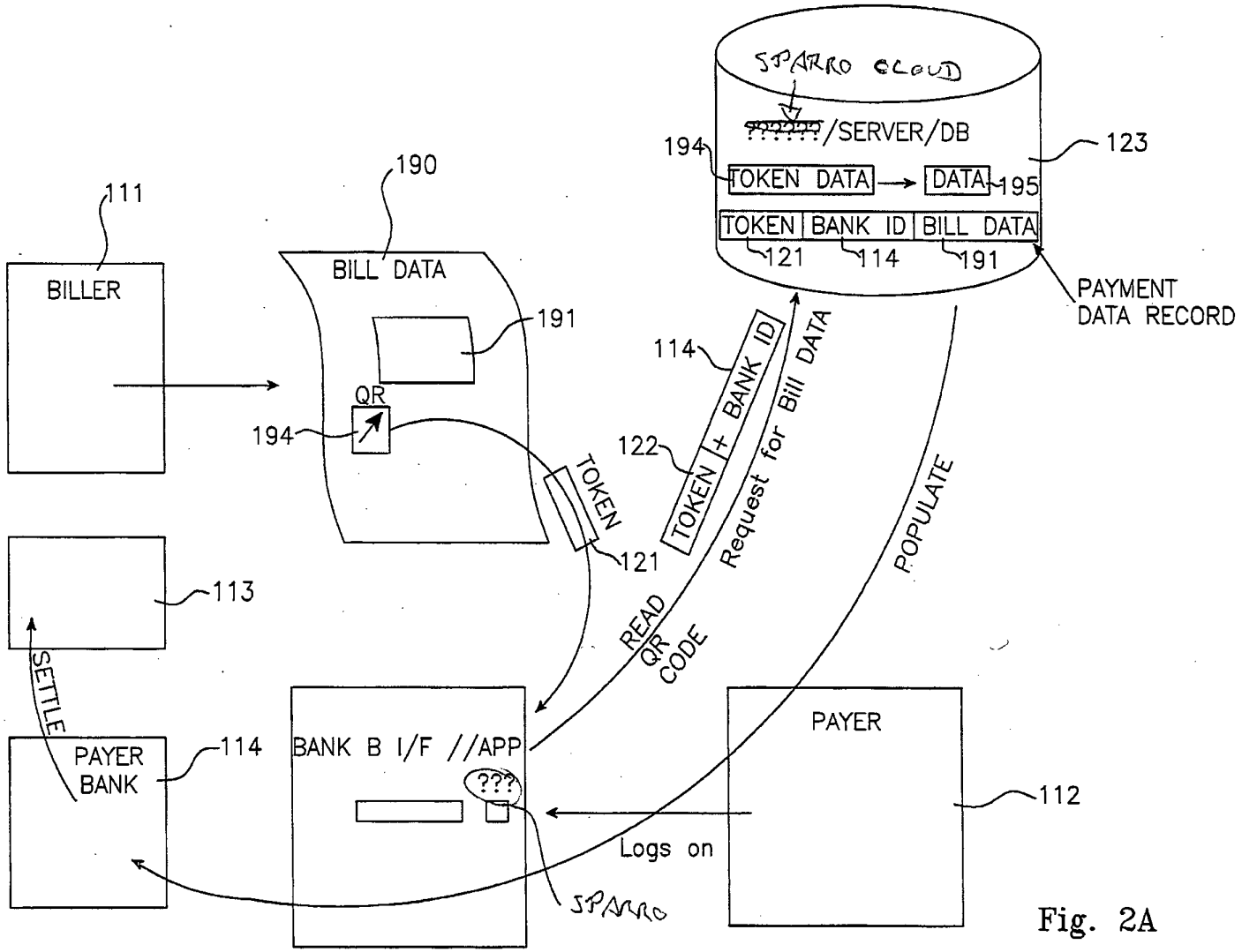

SPARRO cloud
/SERVER/DB
123
194
TOKEN DATA
DATA
195
TOKEN
BANK ID
BILL DATA
121
114
191
PAYMENT DATA RECORD
111
BILLER
190
BILL DATA
191
QR
194
TOKEN
121
114
BANK ID
122
TOKEN
Request for Bill DATA
POPULATE
READ QR CODE
113
SETTLE
PAYER BANK
114
BANK B I/F //APP
???
PAYER
112
Logs on
SPARRO

Fig. 2A

3/13

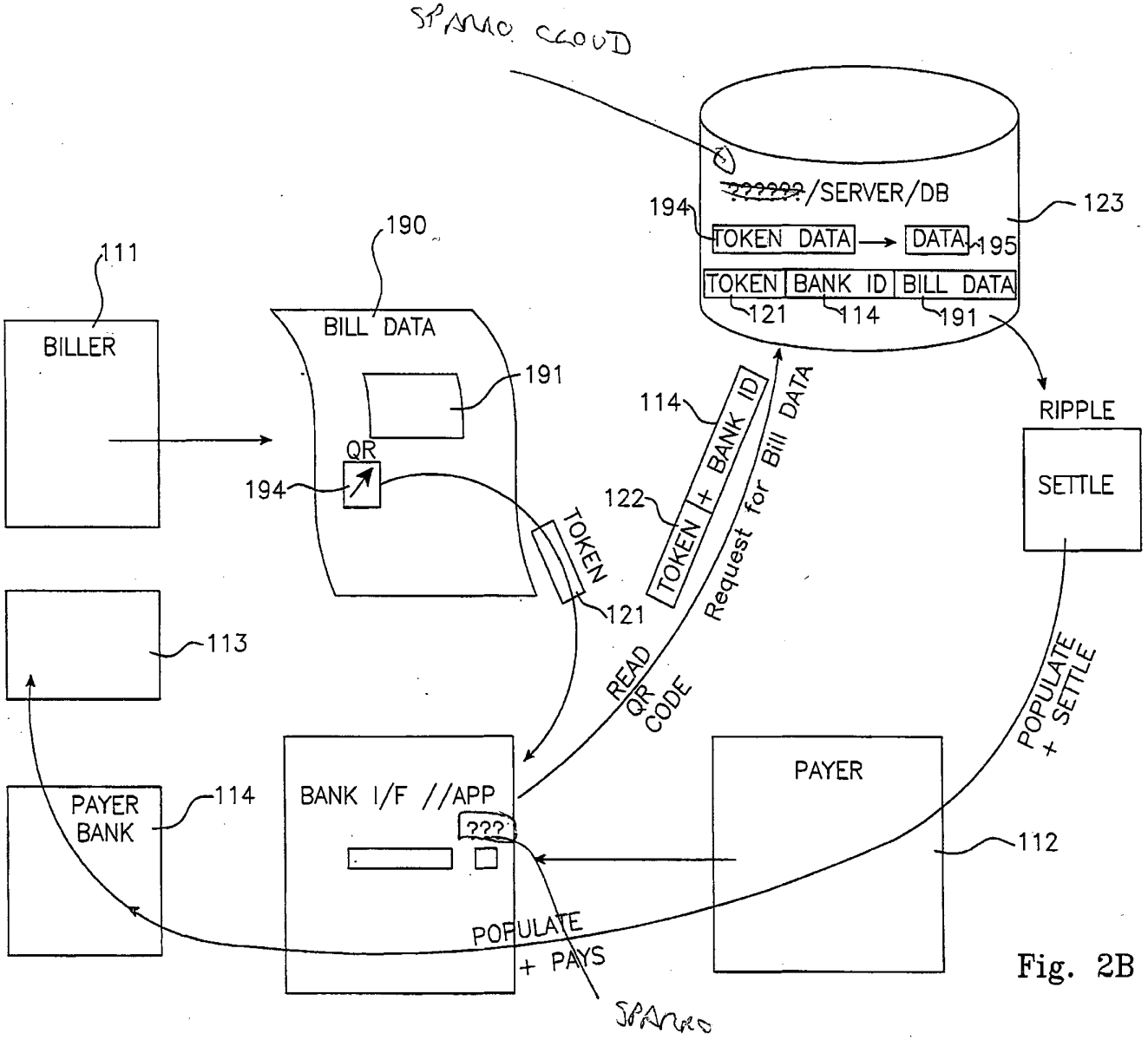

SPARO CLOUD
??????/SERVER/DB
123
194
TOKEN DATA
DATA
195
TOKEN
BANK ID
BILL DATA
121
114
191
111
BILLER
190
BILL DATA
191
QR
194
TOKEN
121
114
+ BANK ID
122
TOKEN
Request for Bill DATA
RIPPLE
SETTLE
113
READ QR CODE
POPULATE + SETTLE
PAYER BANK
114
BANK I/F //APP
???
PAYER
112
POPULATE + PAYS
SPARO

Fig. 2B

4/13

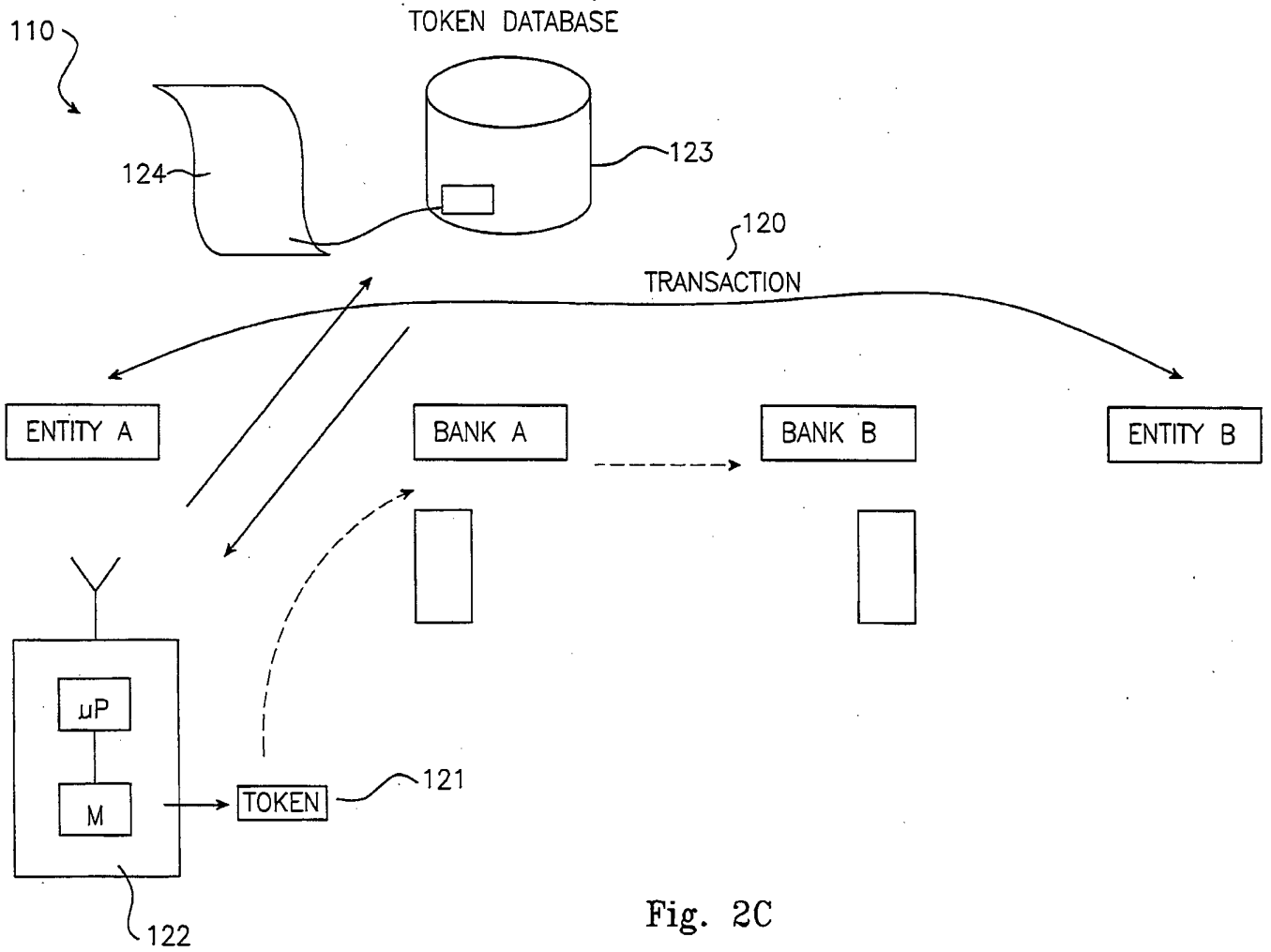

110
TOKEN DATABASE
124
123
120
TRANSACTION
ENTITY A
BANK A
BANK B
ENTITY B
μP
M
TOKEN
121
122

Fig. 2C

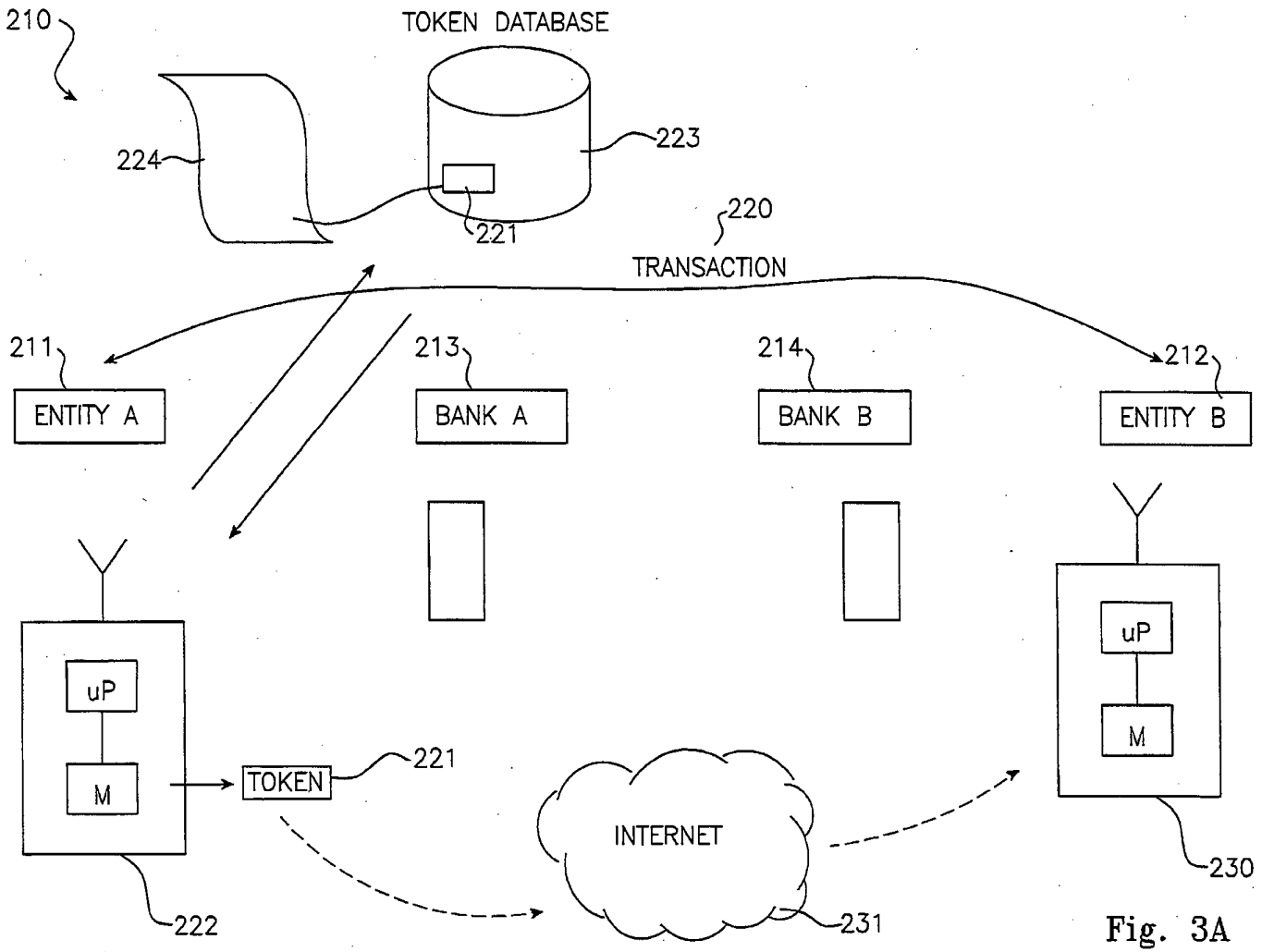

210
TOKEN DATABASE
224
223
221
220
TRANSACTION
211
213
214
212
ENTITY A
BANK A
BANK B
ENTITY B
uP
M
TOKEN
221
INTERNET
230
222
231

Fig. 3A

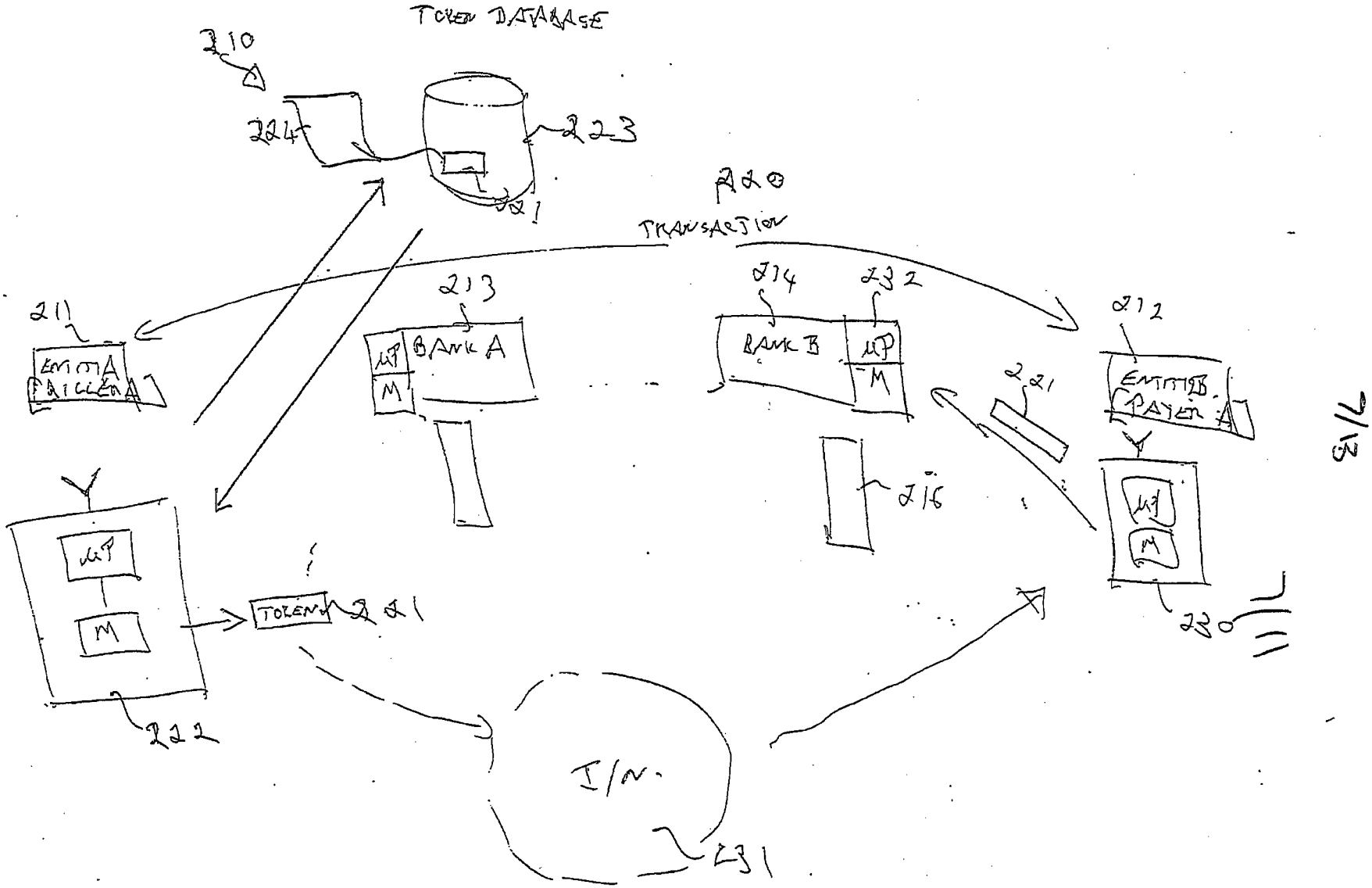

TOKEN DATABASE
210
224
223
221
220
TRANSACTION
211
EMITTER PAYER A
213
BANK A
MP
M
214
232
BANK B
MP
M
231
212
EMITTER PAYER B
MP
M
216
TOKEN
241
222
220
I/N.
231

Fig 3B

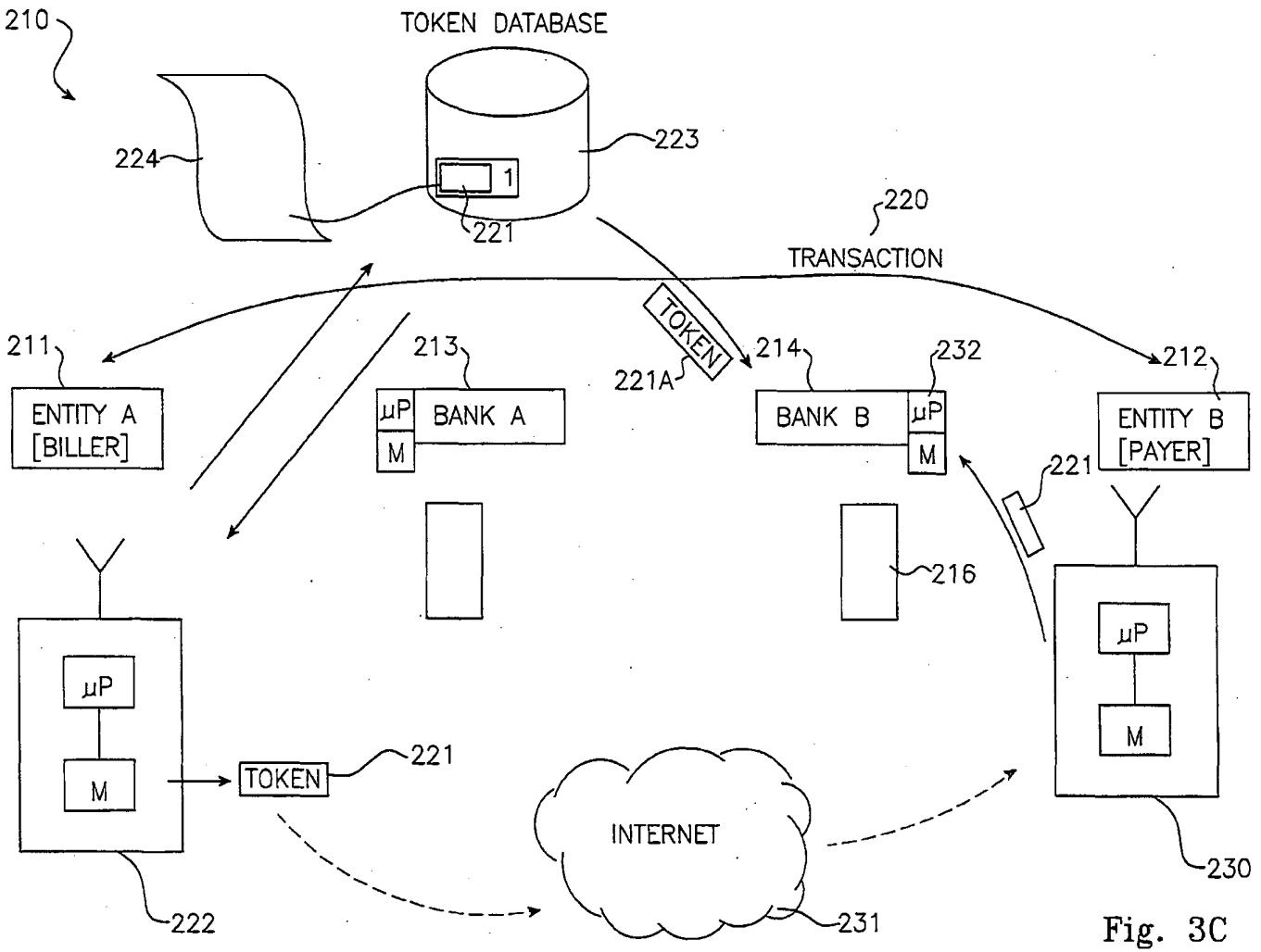
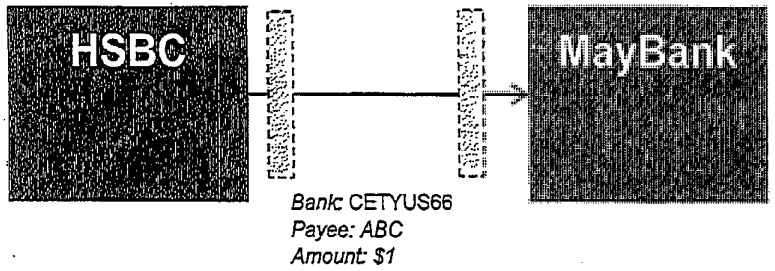

210
TOKEN DATABASE
224
223
1
221
220
TRANSACTION
TOKEN
221A
211
ENTITY A
[BILLER]
213
μP
BANK A
M
214
232
BANK B
μP
M
212
ENTITY B
[PAYER]
221
216
μP
M
TOKEN
221
INTERNET
μP
M
230
222
231

Fig. 3C

8/13

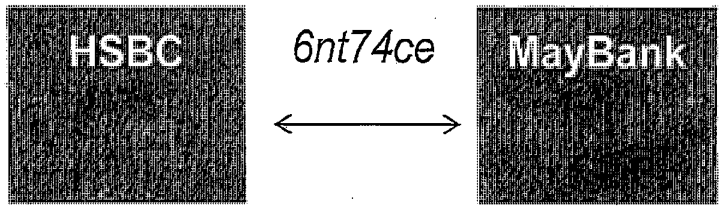
Our token system gives power back to Banks run their own shop; with their own, decentralized security management

Existing (SWIFT) system



(a) Depends on SWIFT infrastructure

Proposed system



(a) Bank-originating (cuts costs)

(b) Optional add-on: Data-enriched for PaaS for customers

fig 4.

1. Specific to transaction 2. SWIFT codes based on correspondent identifiers, so anyone can do it

We can curate our messaging system to accommodate Bank's risk appetite in relation to user data

Base case	Option A: XX	Option B: Data rich
Fully anonymized data	**Text** • Text - Text	**User ID shared with Sparro**
Bank-powered • Tokenization within bank • User ID generation in banks		**Bank-powered** • Tokenization within bank • User ID generation in banks
Benefit • Processing cost • Improved confidentiality of transaction data		**Benefit** • Processing costs • Enriched Payments as a Service to Bank customers

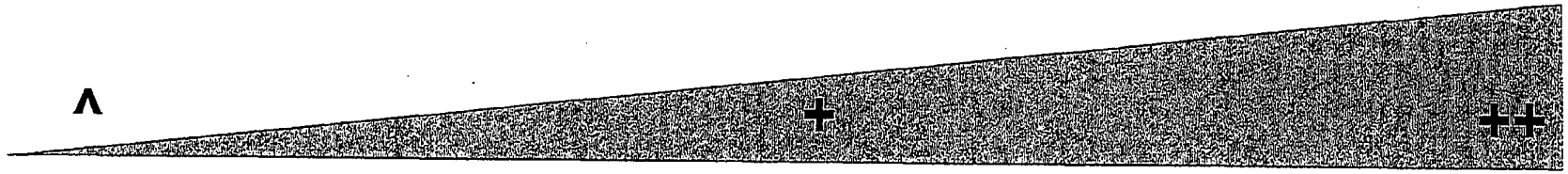
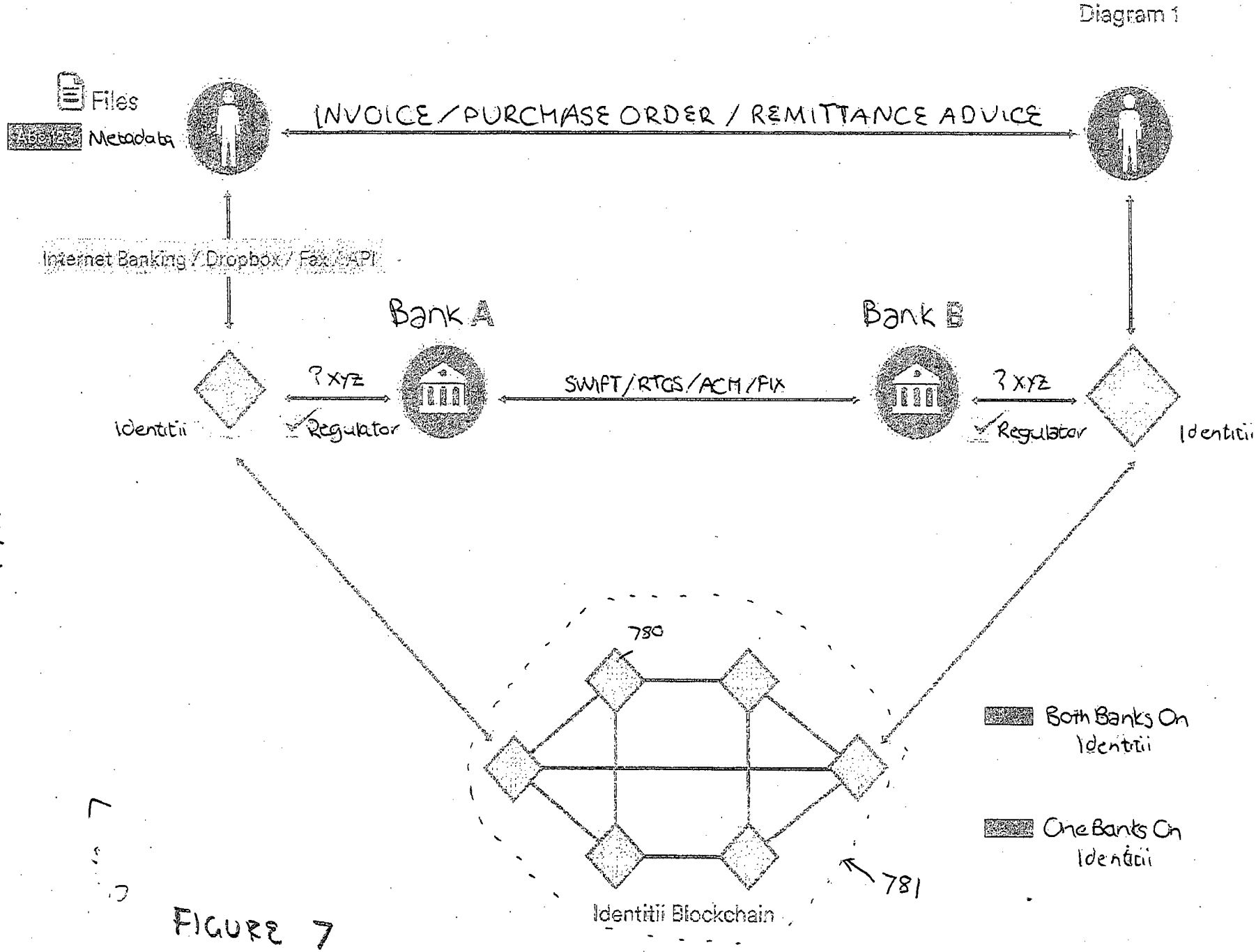


Fig 5

SUMMARY: Benefits to Banks vis-a-vis SWIFT and Ripple

Issue	SWIFT	Ripple	Proposed
Commercial	Bypass SWIFT	No competition, given infrastructure focus	1. Banks turn cost centre re SWIFT processing into profit pool 2. *Optional add-on:* new revenue from e.g. PaaS
Security	SWIFT-based	Block chain	1. Bank's private system
Technical	Committed infrastructure spend is slow & expensive	Private gateway establishment	Sparro (anonymized) messaging

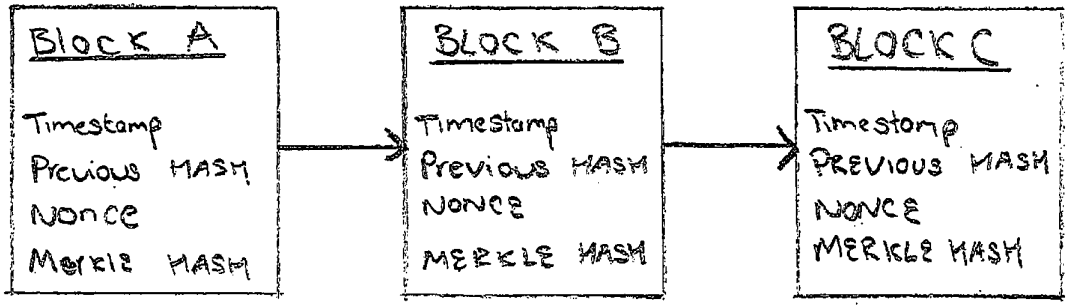
fig 6.



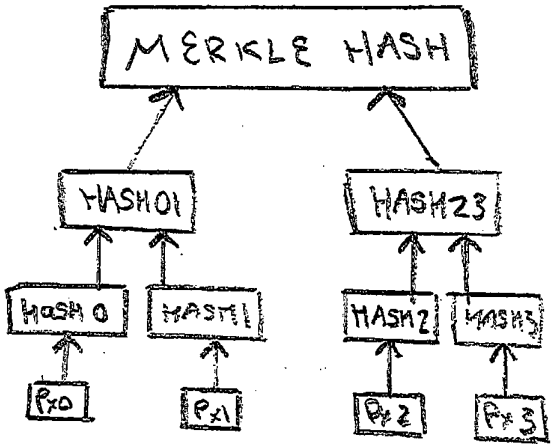
12/13

FIGURE 7

FIGURE 8



Where



WIPO
WORLD
INTELLECTUAL PROPERTY
ORGANIZATION

DOCUMENT MADE AVAILABLE UNDER THE PATENT COOPERATION TREATY (PCT)

International application number:		**PCT/AU2016/000279**
International filing date:		**12 August 2016 (12.08.2016)**
Document type:		**Certified copy of priority document**
Document details:	Country/Office:	**AU**
	Number:	**2016900239**
	Filing date:	**27 January 2016 (27.01.2016)**
Date of receipt at the International Bureau:		**27 September 2016 (27.09.2016)**

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a),(b) or (b-*bis*)

34, chemin des Colombettes
1211 Geneva 20, Switzerland
www.wipo.int

U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE		ATTORNEY DOCKET NUMBER AMK-5243-0009
TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371		U.S. APPLICATION NO. (If known, see 37 C.F.R. 1.5)
INTERNATIONAL APPLICATION NO. PCT/AU2016/000279	INTERNATIONAL FILING DATE 08/12/2016	PRIORITY DATE CLAIMED 08/14/2015
TITLE OF INVENTION		CONFIRMATION NO.:
COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR		
FIRST NAMED INVENTOR		
ARMSTRONG, Nick		

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a submission under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a submission under 35 U.S.C. 371.
3. ☐ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). NOTE: The express request under 35 U.S.C. 371(f) will not be effective unless the requirements under 35 U.S.C. 371(c)(1), (2), and (4) for payment of the basic national fee, copy of the International Application and English translation thereof (if required), and/or the oath or declaration of the inventor(s) have been received.
4. A copy of the International Application as filed (35 U.S.C. 371(c)(2):
   a. ☒ WO 2017/027900 A1 is attached (92 pages specification, claims & abstract (58 claims), 23 sheets drawings).
   b. ☐ has been communicated by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
5. An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)):
   a. ☐ is attached (pages specification, claims & abstract (claims), sheets drawings, page Certificate of Translation).
   b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
6. An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4):
   a. ☐ is attached.
   b. ☐ was previously submitted to the International Bureau during the international phase under PCT Rule 4.17(iv).

Items 7 to 10 below concern amendments made in the international phase

PCT Article 19 and 34 Amendments

7. ☐ Amendments to the claims of the International Application under PCT Article 19 are attached (required only if not communicated by the International Bureau). (35 U.S.C. 371(c)(3).
8. ☐ English language translation of the amendments to the claims under PCT Article 19 is attached (35 U.S.C. 371(c)(3).
9. ☐ English language translation of the annexes (article 19 and/or 34 amendments only) of the International Preliminary Examination Report is attached (35 U.S.C. 371(c)(5).

Cancellation of Amendments Made in the International Phase

10. Do not enter the amendment made in the international phase:
    a. ☐ under PCT Article 19. ☐ under PCT Article 34.

NOTE: A proper amendment made in English under Article 19 or 34 will be entered in the U.S. national phase application absent a clear instruction from applicant not to enter the amendment(s)

Items 11 to 18 below concern document(s) or information included.

11. ☒ An Information Disclosure Statement under 37 C.F.R. 1.97 and 1.98.
12. ☒ A Preliminary Amendment.
13. ☒ An Application Data Sheet under 37 C.F.R. § 1.76.
14. ☐ A substitute specification. NOTE: A substitute specification cannot include claims. See 37 CFR 1.125(b).
15. ☐ A Power of Attorney and/or change of address letter. ☐ 37 CFR 3.73(c) Statement (when there is an Assignee).
16. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13*ter*.3 and 37 CFR 1.821-1.825.
17. ☐ An assignment document for recording (cover sheet and document(s) if paper filing). Name of Assignee: Identitii Pty Ltd
18. ☒ Other items or information. International Search Report and 4 References

Mail Stop PCT

U.S. APPLN. NO. (If known, see 37 CFR 1.5)	INTERNATIONAL APPLICATION NO. PCT/AU2016/000279	ATTORNEY'S DOCKET NUMBER AMK-5243-0009

☒ The following fees are submitted:

		CALCULATIONS	PTO USE ONLY
	BASIC NATIONAL FEE (37 C.F.R. 1.492(a):		
19. ☒	Basic national fee..... $300.00 (1631)/$150.00 (2631)/$75.00 (3631) PLUS SURCHARGE **IF** Paper Filing (EFF. 11.15.2011)$400.00 (1690)/$200.00 (2690)//$200.00 (3690)	$ 150.00	
20. ☒	Examination Fee..... $ $760.00 (1633)/$380.00 (2633)/$190.00 (3633)	$ 380.00	
21. ☒	Search Fee .....$ ..... $140.00 (1641)/$70.00 (2641)/$35.00 (3641) ..... $520.00 (1642)/$260.00 (2642)/$130.00 (3642) ..... $660.00 (1632)/$330.00 (2632)/$165.00 (3632)	$ 260.00	
	TOTAL OF ABOVE CALCULATIONS	$ **790.00**	
☐	Additional fee for specification and drawings filed in paper over 100 sheets (excluding sequence listing or computer program listing filed in an electronic medium). The fee is $400.00 (1681)/$200.00 (2681)/$100.00 (3681) for each additional 50 sheets of paper or fraction thereof.		

Total Sheets		Extra Sheets		Number of each additional 50 or fraction thereof (round **up** to a whole number)		RATE			
126	-100 =	26	/50 =	0.52		$**400.00** (1681) $**200.00** (2681) $**100.00** (3681)		$	200.00

Surcharge of **$140.00 (1617)/$70.00 (2617)/$35.00 (3617)** for furnishing any of the search fee, examination fee, or the oath or declaration later than ☒ 30 months from the earliest claimed priority date (37 C.F.R. 1.492(h).					$	70.00
CLAIMS	NUMBER FILED		# EXTRA	RATE		
Total Claims	20	minus 20 =	0 X	$100.00 (1615)/$50.00 (2615)/$25.00 (3615)	$	
Independent Claims	3	minus 3 =	0 X	$460.00 (1614)/$230.00 (2614)/$115.00 (3614)	$	
MULTIPLE DEPENDENT CLAIMS(S) (if applicable)				$780.00 (1616)/$390.00 (2616)/$195.00 (3616)	$	
Petition is hereby made to extend the current due date so as to cover the filing date of this paper and attachment(s): One Month Extension $200.00 (1251)/$100.00 (2251)/$50.00 (3251); Two Month Extension $600.00 (1252)/$300.00 (2252)/$150.00 (3252); Three Month Extension $1400.00 (1253)/$700.00 (2253)/$350.00 (3253); Four Month Extension $2200.00 (1254)/$1100.00 (2254)/$550.00 (3254); Five Month Extensions $3000.00 (1255)/$1500.00 (2255)/$750.00 (3255)					$	
☒ Applicant claims small entity status. See 37 CFR 1.27. ☐ Applicant claims "micro entity" status. See 37 CFR 1.29 ☐ Micro entity certification statement filed herewith						
Processing fee of **$140.00 (1618)/$70.00 (2618)/$35.00 (3618)**, for furnishing the English Translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 C.F.R. 1.492(i).						
				TOTAL NATIONAL FEE =	$	**1060.00**
Fee for recording the enclosed assignment (37 C.F.R. 1.21(h). The assignment must be accompanied by an appropriate cover sheet (37 C.F.R. 3.28, 3.31). **$50.00** (8021) /**$0 if filed electronically** per property					$	
Fee for Petition to Revive Unintentionally Abandoned Application;$ **2000.00(1453)/1000.00(2453)/500.00(3453)**					$	
				TOTAL FEES ENCLOSED =	$	**1060.00**
				Amount to be refunded:	$	
				Amount to be Charged:	$	

a. ☒ CREDIT CARD OR DEPOSIT ACCOUNT PAYMENT (CREDIT CARD FORM ATTACHED IF PAPER FILING).
b. ☐ Please charge my Deposit Account No. 14-1140 in the amount of $_____ to cover the above fees.
c. ☒ The Commissioner is hereby authorized to charge any deficiency, or credit any overpayment, in the fee(s) filed, or asserted to be filed, or which should have been filed herewith (or with any paper hereafter filed in this application by this firm) to Deposit Account No. 14-1140. **However, authorization is NOT given hereby to charge any extra claims fee or multiple dependent claims fees.**
d. ☒ The entire content of International Application No. PCT/AU2016/000279 and any U.S. and foreign application(s) corresponding thereto, and AU 2015903292; AU 2016900239; and AU 2016901924, referred to in this application is/are hereby incorporated by reference in this application.

NOTE: Where an appropriate time limit under 37 C.F.R. 1.494 or 1.495 has not been met, a petition to revive (37 C.F.R. 1.137(a) or (b) must be filed and granted to restore the application to pending status.

Mail Stop PCT

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File)Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013, and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.

NOTE: A U.S. national stage application may not claim priority to the international application of which it is the national phase. The filing date of a U.S. national stage application is the international filing date. See 35 U.S.C. 363

CORRESPONDENCE ADDRESS

Direct all correspondence to:

☒ **Customer Number:** **23117**

Type Customer Number here

Telephone: (703) 816-4000

AMK: jls

/Alan M. Kagen/

Alan M. Kagen

NAME

36,178

REGISTRATION NUMBER

February 14, 2018

Date

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	AMK-5243-9
	Application Number	
Title of Invention	COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2:

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Nick		Armstrong	

Residence Information (Select One) US Residency ● Non US Residency Active US Military Service

City	Country of Residence [i]
Sydney	AU

Mailing Address of Inventor:

Address 1	c/o Identitii Pty Ltd
Address 2	Suite 1 Level 3, 66-72 Reservoir St.
City	Surry Hills, New South Wales
State/Province	
Postal Code	2010
Country [i]	AU

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Ben		Buckingham	

Residence Information (Select One) US Residency ◉ Non US Residency Active US Military Service

City	Country of Residence [i]
Sydney	AU

Mailing Address of Inventor:

Address 1	c/o Identitii Pty Ltd
Address 2	Suite 1 Level 3, 66-72 Reservoir St.
City	Surry Hills, New South Wales
State/Province	
Postal Code	2010
Country [i]	AU

Inventor 3 Remove

Legal Name

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	AMK-5243-9
	Application Number	
Title of Invention	COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR	

Prefix	Given Name	Middle Name	Family Name	Suffix
	Daniel		Friedman	

Residence Information (Select One) US Residency ◉ Non US Residency Active US Military Service

City	Sydney	Country of Residence [i]	AU

Mailing Address of Inventor:

Address 1	c/o Identitii Pty Ltd		
Address 2	Suite 1 Level 3, 66-72 Reservoir St.		
City	Surry Hills, New South Wales	State/Province	
Postal Code	2010	Country [i]	AU

Inventor 4 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Elliot		Shepherd	

Residence Information (Select One) US Residency ◉ Non US Residency Active US Military Service

City	Sydney	Country of Residence [i]	AU

Mailing Address of Inventor:

Address 1	c/o Identitii Pty Ltd		
Address 2	Suite 1 Level 3, 66-72 Reservoir St.		
City	Surry Hills, New South Wales	State/Province	
Postal Code	2010	Country [i]	AU

Inventor 5 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Eric		Knight	

Residence Information (Select One) US Residency ◉ Non US Residency Active US Military Service

City	Sydney	Country of Residence [i]	AU

Mailing Address of Inventor:

Address 1	c/o Identitii Pty Ltd		
Address 2	Suite 1 Level 3, 66-72 Reservoir St.		
City	Surry Hills, New South Wales	State/Province	
Postal Code	2010	Country [i]	AU

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	AMK-5243-9
	Application Number	
Title of Invention	COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR	

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below. For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	23117		
Email Address		Add Email	Remove Email

Application Information:

Title of the Invention	COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR		
Attorney Docket Number	AMK-5243-9	**Small Entity Status Claimed**	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	23	**Suggested Figure for Publication (if any)**	

Filing By Reference:

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	AMK-5243-9
	Application Number	
Title of Invention	COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR	

Please Select One:	● Customer Number	US Patent Practitioner	◯ Limited Recognition (37 CFR 11.9)
Customer Number			

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the "Application Number" field blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	a 371 of international	PCTAU2016000279	2016-08-12

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)[i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Remove

Application Number	Country[i]	Filing Date (YYYY-MM-DD)	Access Code[i] (if applicable)
2015903292	AU	2015-08-14	

Remove

Application Number	Country[i]	Filing Date (YYYY-MM-DD)	Access Code[i] (if applicable)
2016900239	AU	2016-01-27	

Remove

Application Number	Country[i]	Filing Date (YYYY-MM-DD)	Access Code[i] (if applicable)
2016901924	AU	2016-05-20	

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	AMK-5243-9
	Application Number	
Title of Invention	COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR	

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	AMK-5243-9
	Application Number	
Title of Invention	COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR	

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

☐ B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	AMK-5243-9
	Application Number	
Title of Invention	COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR	

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1 — Remove

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

● Assignee	Legal Representative under 35 U.S.C. 117	Joint Inventor
Person to whom the inventor is obligated to assign.	Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor:

If the Applicant is an Organization check here. ☒

Organization Name	Identitii Pty Ltd		
Mailing Address Information For Applicant:			
Address 1	Suite 1 Level 3, 66-72 Reservoir St.		
Address 2			
City	Surry Hills, New South Wales	**State/Province**	
Country	AU	Postal Code	2010
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	AMK-5243-9
	Application Number	
Title of Invention	COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR	

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

Remove

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add

Signature:

Remove

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). **However, if this Application Data Sheet is submitted with the INITIAL filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).**

This Application Data Sheet must be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/Alan M. Kagen/			Date (YYYY-MM-DD)	2018-02-14
First Name	Alan	Last Name	Kagen	Registration Number	36178

Additional Signature may be generated within this form by selecting the Add button. Add

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	AMK-5243-9
	Application Number	
Title of Invention	COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR	

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1 The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3 A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent CooperationTreaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 February 2017 (23.02.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/027900 A1

(51) International Patent Classification:
G06Q 20/38 (2012.01) *G06F 17/30* (2006.01)

(21) International Application Number:
PCT/AU2016/000279

(22) International Filing Date:
12 August 2016 (12.08.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

2015903292	14 August 2015 (14.08.2015)	AU
2016900239	27 January 2016 (27.01.2016)	AU
2016901924	20 May 2016 (20.05.2016)	AU

(71) Applicant: **IDENTITII PTY LTD** [AU/AU]; Suite 1 Level 3, 66-72 Reservoir St., Surry Hills, New South Wales 2010 (AU).

(72) Inventors: **ARMSTRONG, Nick**; Suite 1 Level 3, 66-72 Reservoir St., Surry Hills, New South Wales 2010 (AU). **BUCKINGHAM, Ben**; Suite 1 Level 3, 66-72 Reservoir St, Surry Hills, New South Wales 2010 (AU). **FRIEDMAN, Daniel**; Suite 1 Level 3, 66-72 Reservoir St., Surry Hills, New South Wales 2010 (AU). **SHEPHERD, Elliot**; Suite 1 Level 3, 66-72 Reservoir St, Surry Hills, New South Wales 2010 (AU). **KNIGHT, Eric**; Suite 1 Level 3, 66-72 Reservoir St, Surry Hills, New South Wales 2010 (AU).

(74) Agent: **BAXTER PATENT ATTORNEYS PTY LTD**; Suite 2, Level 3A, 1 Bligh St, Sydney, New South Wales 2000 (AU).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) Title: A COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR

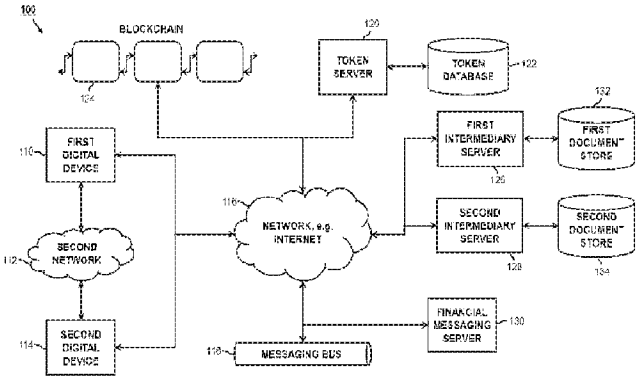


FIG. 1

(57) Abstract: The present invention provides a computer implemented method for processing a financial transaction, the method comprising the steps of transmitting one or more documents pertaining to the financial transaction, from a first intermediary server to a first document store, generating an enriched data record from the one or more documents, at the first intermediary server, and adding the enriched data record into a blockchain, from the first intermediary sever, requesting generation of a token corresponding to the financial transaction, to a token server, from the first intermediary server, via a messaging bus, generating the token at the token server and adding the token into the blockchain from the token server, transmitting the token to the first intermediary server from the token server, via the messaging bus and transmitting the token from the first intermediary server to the first document store.

WO 2017/027900 A1

A COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR

Field of the Invention

[001] The present invention relates to financial transactions and in particular to a method and a system for processing a financial transaction.

[002] The invention has been developed primarily for use in/with financial transactions and will be described hereinafter with reference to this application. However, it will be appreciated that the invention is not limited to this particular field of use.

Background of the Invention

[003] A financial transaction comprises at least two parties, with a transfer of currency taking place between the two parties. The currency may include electronic currency and fiat currency. In either case, any financial transaction includes a plurality of data associated with the financial transaction. The plurality of data may include payment metadata such as account numbers of the at least two parties, Business Identifier Codes (BIC) of the financial institutions corresponding to the at least two parties, amount of currency to be transferred and type of currency etc. Further, the plurality of data may include regulatory compliance documents such as KYC documents.

[004] Generally, it is difficult to keep track of the plurality of data during the financial transaction. Further, it is even more difficult to ensure that integrity of the plurality of data is maintained either during or after the financial transaction has been completed or to evidence that it existed at a certain point in the financial transaction process. Many settlement systems are characterised by effective one-way transmission of the plurality of data in any given financial transaction (for example systems based on SWIFT messaging). If it is subsequently discovered that there are deficiencies in the plurality of data transmitted, time consuming checking and querying operations and correspondence often ensues before the financial transaction can be effected.

[005] Therefore there remains, in the art, a need for improved methods and systems for processing a financial transaction which do not suffer from the above mentioned issues.

[006] Any discussion of the background art throughout the specification should in no way be considered as an admission that such background art is prior art, nor that such background art is widely known or forms part of the common general knowledge in the field in Australia or any other country.

Summary of the Invention

[007] According to a first aspect of the present invention, there is provided a computer implemented method for processing a financial transaction, the method comprising the steps of transmitting one or more documents pertaining to the financial transaction, from a first intermediary server to a first document store, generating an enriched data record from the one or more documents, at the first intermediary server, and adding the enriched data record into a blockchain, from the first intermediary sever, requesting generation of a token corresponding to the financial transaction, to a token server, from the first intermediary server, via a messaging bus, generating the token at the token server and adding the token into the blockchain from the token server, transmitting the token to the first intermediary server from the token server, via the messaging bus and transmitting the token from the first intermediary server to the first document store. The token provides a pointer to the enriched data record in the blockchain. Thus the token can used to retrieve the enriched data record at a time of an audit.

[008] In one embodiment of the invention, the computer implemented method further comprises the step of sending a first financial message comprising the token, from the first intermediary server to a second intermediary server, indicative of making a payment to a second user.

[009] In one embodiment of the invention, the computer implemented method further comprises the steps of implementing a smart contract at the token server; and adding the smart contract into the blockchain, from the token server.

[010] In one embodiment of the invention, the computer implemented method further comprises the steps of transmitting the token from the first intermediary server to a first digital device available with a first user, providing the token to a second user, by the first user, providing the token to a second intermediary server, from the second digital device, transmitting the token to a second document store, from the second intermediary server and sending a second financial message comprising the token, from the second intermediary server to the first intermediary server, indicative of making a payment to the first user.

[011] In one embodiment of the invention, the step of generating the enriched data record comprises extracting a plurality of attributes from the one or more documents, at the first intermediary server and combining the plurality of attributes to generate the enriched data record, at the first intermediary server.

[012] In one embodiment of the invention, the step of generating the enriched data record comprises extracting a plurality of attributes from the one or more documents, at the first intermediary server, de-identifying the plurality of attributes to obtain a plurality of de-identified attributes, at the first intermediary server and combining the plurality of de-identified attributes to generate the enriched data record, at the first intermediary server. De-identification of the plurality of attributes ensures that confidentiality of any person or entity involved in the financial transaction is not compromised during a hacking attack on the blockchain.

[013] In one embodiment of the invention, the step of generating the enriched data record comprises extracting a plurality of attributes from the one or more documents, at the first intermediary server, hashing the plurality of attributes to generate a plurality of respective hashes, at the first intermediary server and combining the plurality of hashes to generate the enriched data record, at the first intermediary server. Hashing provides even more protection against tampering of theft, to the one or more documents, as the hashes are irreversible.

[014] In one embodiment of the invention, the computer implemented method further comprises the step of assigning a payment risk rating to the token. The payment risk rating is a direct measure of the regulatory and other compliance checks involved in the financial transaction.

[015] In one embodiment of the invention, the computer implemented method further comprises the steps of transmitting one or more first requests, each comprising the token, from the first intermediary server to the second intermediary server, via the messaging bus, receiving the one or more first requests at the second intermediary server and transmitting the one or more first requests and the token from the second intermediary server to a second document store, generating one or more first responses, each comprising the token, corresponding to the respective one or more first requests, at the second intermediary server, transmitting the one or more first responses from the second intermediary server to the first intermediary server, via the messaging bus, hashing the one or more first requests and the one or more first responses at the second intermediary server to generate one or more first request hashes and one or more first response hashes, respectively, adding the one or more first request hashes and the one or more first response hashes to the enriched data record in the blockchain, from the second intermediary server and receiving the one or more first responses at the first intermediary server and transmitting the one or more first responses to the first document store. This communication between the first intermediary server and the second intermediary server allows the first intermediary server to execute all the necessary compliance checks.

[016] In one embodiment of the invention, the computer implemented method further comprises the steps of hashing the one or more first responses at the first intermediary server to regenerate the one or more first response hashes and verifying the one or more first response hashes with the blockchain from the first intermediary server, using the token. Thus, the integrity of the one or more first responses can be verified with the blockchain, at any given time.

[017] In one embodiment of the invention, each one of the one or more first requests are encrypted with a second public key and signed with a first public

key at the first intermediary server, before transmission to the second intermediary server and decrypted with a second private key at the second intermediary server after reception from the first intermediary server. Further, each one of the one or more first responses are encrypted with the first public key and signed with the second public key at the second intermediary server, before transmission to the first intermediary server and decrypted with a first private key at the first intermediary server after reception from the second intermediary server. Using pairs of asymmetrical keys ensures that the requests and the responses are not intercepted during transmission.

[018] In one embodiment of the invention, the one or more first responses comprise one or more second regulatory compliance documents pertaining to a second user.

[019] In one embodiment of the invention, the computer implemented method further comprises the steps of transmitting one or more second requests, each comprising the token, from the second intermediary server to the first intermediary server, via the messaging bus, receiving the one or more second requests at the first intermediary server and transmitting the one or more second requests from the first intermediary server to the first document store, generating one or more second responses, each comprising the token, corresponding to the respective one or more second requests, at the first intermediary server, transmitting the one or more second responses from the first intermediary server to the second intermediary server, via the messaging bus, hashing the one or more second requests and the one or more second responses at the first intermediary server to generate one or more second request hashes and one or more second response hashes, respectively, adding the one or more second request hashes and the one or more second response hashes to the enriched data record in the blockchain, from the first intermediary server and receiving the one or more second responses at the second intermediary server and transmitting the one or more second responses to the second document store. This communication enables the second intermediary server to execute all the necessary compliance checks.

[020] In one embodiment of the invention, the computer implemented method further comprises the steps of hashing the one or more second responses at the second intermediary server to regenerate the one or more second response hashes and verifying the one or more second response hashes with the blockchain from the second intermediary server, using the token. Similar to one or more first responses, the integrity of the one or more second responses can be verified with the blockchain, at any given time.

[021] In one embodiment of the invention, each one of the one or more second requests are encrypted with a first public key and signed with a second public key at the second intermediary server, before transmission to the first intermediary server and decrypted with a first private key at the first intermediary server after reception from the second intermediary server. Further, each one of the one or more second responses are encrypted with the second public key and signed with the first public key at the first intermediary server, before transmission to the second intermediary server and decrypted with a second private key at the second intermediary server after reception from the first intermediary server. Using pairs of asymmetrical keys ensures that the requests and the responses are not intercepted during transmission.

[022] In one embodiment of the invention, the computer implemented method further comprises the steps of adding the first public key from the first intermediary server into the blockchain and adding the second public key from the second intermediary server into the blockchain.

[023] In one embodiment of the invention, the one or more second responses comprise one or more first regulatory compliance documents pertaining to a first user.

[024] According to a second aspect of the present invention, there is provided a system for processing a financial transaction, the system comprising a first intermediary server operably connected to a network and a first document store, a token server operably connected to the network, a messaging bus operably connected to the network and a blockchain operably connected to the network.

Further, the first intermediary server is configured to transmit one or more documents pertaining to the financial transaction, to the first document store, generate an enriched data record from the one or more documents and add the enriched data record into the blockchain, request generation of a token corresponding to the financial transaction, to the token server, via the messaging bus and transmit the token to the first document store. Further, the token server is configured to generate the token and add the token into the blockchain and transmit the token to the first intermediary server, via the messaging bus.

[025] In one embodiment of the invention, the system further comprises a second intermediary server operably connected to the network and a second document store. Further, the first intermediary server is further configured to send a first financial message comprising the token, to the second intermediary server, indicative of making a payment to a second user.

[026] In one embodiment of the invention, the token server is further configured to implement a smart contract and add the smart contract into the blockchain.

[027] In one embodiment of the invention, the system further comprises a first digital device operably connected to the network, a second digital device operably connected to the network, a second intermediary server operably connected to the network and a second document store. Further, the first intermediary server is further configured to transmit the token to the first digital device. Further, the first digital device comprises a first memory and a first processor operably connected to the first memory, the first memory comprising a first computer program code, the first computer program code when executed by the first processor, instructs the first processor to receive the token from the first intermediary server, provide the token to the second digital device. Further, the second digital device comprises a second memory and a second processor operably connected to the second memory, the second memory comprising a second computer program code, the second computer program code when executed by the second processor, instructs the second processor to receive the token from the first digital device and provide the token to the second intermediary server. Also, the second intermediary server is configured to receive

the token from the second digital device, transmit the token to the second document store and send a second financial message comprising the token, to the first intermediary server, indicative of making a payment to a first user.

[028] In one embodiment of the invention, for generation of the enriched data record, the first intermediary server is configured to extract a plurality of attributes from the one or more documents and combine the plurality of attributes to generate the enriched data record.

[029] In one embodiment of the invention, for generation of the enriched data record, the first intermediary server is configured to extract a plurality of attributes from the one or more documents, de-identify the plurality of attributes to obtain a plurality of de-identified attributes and combine the plurality of de-identified attributes to generate the enriched data record.

[030] In one embodiment of the invention, for generation of the enriched data record, the first intermediary server is configured to extract a plurality of attributes from the one or more documents, hash the plurality of attributes to generate a plurality of respective hashes and combine the plurality of hashes to generate the enriched data record.

[031] In one embodiment of the invention, the first intermediary server is further configured to assign a payment risk rating to the token.

[032] In one embodiment of the invention, the system further comprises a second intermediary server operably connected to the network and a second document store. Further, the first intermediary server is configured to transmit one or more first requests, each comprising the token, to the second intermediary server, via the messaging bus and receive one or more first responses and transmit the one or more first responses to the first document store. Further, the second intermediary server is configured to receive the one or more first requests from the first intermediary server and transmit the one or more first requests and the token to the second document store, generate the one or more first responses, each comprising the token, corresponding to the respective one or more first

requests, transmit the one or more first responses to the first intermediary server, via the messaging bus, hash the one or more first requests and the one or more first responses to generate one or more first request hashes and one or more first response hashes, respectively and add the one or more first request hashes and the one or more first response hashes to the enriched data record in the blockchain.

[033] In one embodiment of the invention, the first intermediary server is further configured to hash the one or more first responses to regenerate the one or more first response hashes and verify the one or more first response hashes with the blockchain, using the token.

[034] In one embodiment of the invention, the first intermediary server is further configured to encrypt each one of the one or more first requests with a second public key and sign each one of the one or more first requests with a first public key, before transmission to the second intermediary server and decrypt each one of the one or more first responses with a first private key after reception from the second intermediary server. Further, the second intermediary server is further configured to encrypt the each one of the one or more first responses with the first public key and sign the each one of the one or more first responses with the second public key, before transmission to the first intermediary server and decrypt the each one of the one or more first requests with a second private key after reception from the first intermediary server.

[035] In one embodiment of the invention, the one or more first responses comprise one or more second regulatory compliance documents pertaining to a second user.

[036] In one embodiment of the invention, the system further comprises a second intermediary server connected to the network and a second document store. Further, the second intermediary server is configured to transmit one or more second requests, each comprising the token, to the first intermediary server, via the messaging bus, receive one or more second responses and transmit the one or more second responses to the second document store. Further, the first

intermediary server is further configured to receive the one or more second requests and transmit the one or more second requests to the first document store, generate the one or more second responses, each comprising the token, corresponding to the respective one or more second requests, transmit the one or more second responses to the second intermediary server, via the messaging bus, hash the one or more second requests and the one or more second responses to generate one or more second request hashes and one or more second response hashes, respectively and add the one or more second request hashes and the one or more second response hashes to the enriched data record in the blockchain.

[037] In one embodiment of the invention, the second intermediary server is further configured to hash the one or more second responses to regenerate the one or more second response hashes and verify the one or more second response hashes with the blockchain, using the token.

[038] In one embodiment of the invention, the second intermediary server is further configured to encrypt each one of the one or more second requests with a first public key and sign each one of the one or more second requests with a second public key, before transmission to the first intermediary server and decrypt each one of the one or more second responses with a second private key after reception from the first intermediary server. Further, the first intermediary server is further configured to encrypt the each one of the one or more second responses with the second public key and sign the each one of the one or more second responses with the first public key, before transmission to the second intermediary server and decrypt the each one of the one or more second requests with a first private key after reception from the second intermediary server.

[039] In one embodiment of the invention, the first intermediary server is further configured to add the first public key into the blockchain and the second intermediary server is further configured to add the second public key into the blockchain.

[040] In one embodiment of the invention, the one or more second responses comprise one or more first regulatory compliance documents pertaining to a first user.

[041] According to a third aspect of the present invention, there is provided a token server for facilitating processing of a financial transaction, operably connected to a network and configured to generate a token, add the token into a blockchain and transmit the token to a first intermediary server, via a messaging bus.

[042] In one embodiment of the invention, the token server is further configured to implement a smart contract and add the smart contract into the blockchain.

[043] According to a fourth aspect of the present invention, there is provided a first intermediary server for facilitating processing of a financial transaction, operably connected to a network and a first document store, and configured to transmit one or more documents pertaining to the financial transaction, to the first document store, generate an enriched data record from the one or more documents and add the enriched data record into a blockchain, request generation of a token corresponding to the financial transaction, to a token server, via a messaging bus and transmit the token to the first document store.

[044] In one embodiment of the invention, the first intermediary server is further configured to send a first financial message comprising the token, to a second intermediary server, indicative of making a payment to a second user.

[045] In one embodiment of the invention, the first intermediary server is further configured to transmit the token to a first digital device.

[046] In one embodiment of the invention, for generation of the enriched data record, the first intermediary server is configured to extract a plurality of attributes from the one or more documents and combine the plurality of attributes to generate the enriched data record.

[047] In one embodiment of the invention, for generation of the enriched data record, the first intermediary server is configured extract a plurality of attributes from the one or more documents, de-identify the plurality of attributes to obtain a plurality of de-identified attributes and combine the plurality of de-identified attributes to generate the enriched data record.

[048] In one embodiment of the invention, for generation of the enriched data record, the first intermediary server is configured to extract a plurality of attributes from the one or more documents, hash the plurality of attributes to generate a plurality of respective hashes and combine the plurality of hashes to generate the enriched data record.

[049] In one embodiment of the invention, the first intermediary server is further configured to assign a payment risk rating to the token.

[050] In one embodiment of the invention, the first intermediary server is further configured to transmit one or more first requests, each comprising the token, to a second intermediary server, via the messaging bus and receive one or more first responses from the second intermediary server and transmit the one or more first responses to the first document store.

[051] In one embodiment of the invention, the one or more first responses comprise one or more second regulatory compliance documents pertaining to a second user.

[052] In one embodiment of the invention, the first intermediary server is further configured to hash the one or more first responses to regenerate one or more first response hashes and verify the one or more first response hashes with the blockchain, using the token.

[053] In one embodiment of the invention, the first intermediary server is further configured to encrypt each one of the one or more first requests with a second public key and sign each one of the one or more first requests with a first public

key, before transmission to the second intermediary server and decrypt each one of the one or more first responses with a first private key after reception from the second intermediary server.

[054] In one embodiment of the invention, the first intermediary server is further configured to receive the one or more second requests from a second intermediary server and transmit the one or more second requests to the first document store, generate one or more second responses, each comprising the token, corresponding to the respective one or more second requests, transmit the one or more second responses to the second intermediary server, via the messaging bus, hash the one or more second requests and the one or more second responses to generate one or more second request hashes and one or more second response hashes, respectively and add the one or more second request hashes and the one or more second response hashes to the enriched data record in the blockchain.

[055] In one embodiment of the invention, the first intermediary server is further configured to encrypt each one of the one or more second responses with a second public key and sign the each one of the one or more second responses with a first public key, before transmission to the second intermediary server and decrypt each one of the one or more second requests with a first private key after reception from the second intermediary server.

[056] In one embodiment of the invention, the first intermediary server is further configured to add the first public key into the blockchain.

[057] According to a fifth aspect of the present invention, there is provided a second intermediary server for facilitating processing of a financial transaction, operably connected to a network and a second document store, and configured to receive the token from the second digital device, transmit the token to the second document store and send a second financial message comprising the token to a first intermediary server, indicative of making a payment to a first user.

[058] According to a sixth aspect of the present invention, there is provided a second intermediary server for facilitating processing of a financial transaction, operably connected to a network and a second document store, and configured to receive one or more first requests, each comprising a token, from a first intermediary server and transmit the one or more first requests and the token to the second document store, generate the one or more first responses, each comprising the token, corresponding to the respective one or more first requests, transmit the one or more first responses to the first intermediary server, via a messaging bus, hash the one or more first requests and the one or more first responses to generate one or more first request hashes and one or more first response hashes, respectively and add the one or more first request hashes and the one or more first response hashes to the enriched data record in the blockchain.

[059] In one embodiment of the invention, the second intermediary server is further configured to encrypt each one of the one or more first responses with a first public key and sign the each one of the one or more first responses with a second public key, before transmission to the first intermediary server and decrypt each one of the one or more first requests with a second private key after reception from the first intermediary server.

[060] According to a seventh aspect of the invention, there is provided a second intermediary server for facilitating processing of a financial transaction, operably connected to a network and a second document store, and configured to transmit one or more second requests, each comprising a token, to a first intermediary server, via a messaging bus and receive one or more second responses from the first intermediary server and transmit the one or more second responses to the second document store.

[061] In one embodiment of the invention, the second intermediary server is further configured to hash the one or more second responses to regenerate one or more second response hashes and verify the one or more second response hashes with the blockchain, using the token.

[062] In one embodiment of the invention, the second intermediary server is further configured to encrypt each one of the one or more second requests with a first public key and sign each one of the one or more second requests with a second public key, before transmission to the first intermediary server and decrypt each one of the one or more second responses with a second private key after reception from the first intermediary server.

[063] In one embodiment of the invention, the second intermediary server is further configured to add the second public key into the blockchain.

[064] In one embodiment of the invention, the one or more second responses comprise one or more first regulatory compliance documents pertaining to a first user.

[065] Other aspects of the invention are also disclosed.

Brief Description of the Drawings

[066] Notwithstanding any other forms which may fall within the scope of the present invention, a preferred embodiment / preferred embodiments of the invention will now be described, by way of example only, with reference to the accompanying drawings in which:

[067] Fig. 1 illustrates a top level diagram of a system of computing devices to which various embodiments described herein may be implemented;

[068] Fig. 2 illustrates a subsystem of the computing devices for generation of a token, in accordance with a preferred embodiment of the present invention;

[069] Fig. 3 illustrates a subsystem of the computing devices for exchange of requests and responses between two intermediary servers, via a messaging bus, in accordance with a preferred embodiment of the present invention;

[070] Fig. 4 illustrates a subsystem of the computing devices for making a payment to a second user, by a first user, in accordance with a preferred embodiment of the present invention;

[071] Fig. 5 illustrates a subsystem of the computing devices for making a payment to the first user, by the second user, in accordance with a preferred embodiment of the present invention;

[072] Fig. 6 illustrates a computing device to which various embodiments described herein may be implemented; and

[073] Fig. 7 illustrates a computer implemented method for processing a financial transaction, in accordance with a preferred embodiment of the present invention;

[074] Figure 8A is a block diagram of the entities and intermediaries involved in a prior art electronic settlement system;

[075] Figure 8B is a data and funds flow according to a prior art settlement system;

[076] Figure 9A, 9B is a data and funds flow diagram according to an indicative embodiment of the present invention;

[077] Figure 9C is a block diagram of the basic infrastructure and components suited for use with embodiments of the present invention;

[078] Figure 10 A, B, C comprise block diagrams of the steps in a settlement transaction in accordance with a first preferred embodiment of the present invention;

[079] Figure 11 is a block diagram of salient characteristics of a messaging system 810 of the prior art as compared with the salient messaging characteristics of the system 1010 enabled by the code of a second embodiment;

[080] Figure 12 illustrates the options for data content to be included in tokens in accordance with embodiments of the invention as described above;

[081] Figure 13 provides a comparison of characteristics of embodiments of the present invention as compared with the prior art Swift-based messaging system;

[082] Figure 14 is a block diagram in accordance with a further preferred embodiment of the present invention;

[083] Figures 15A and15B are block diagrams of an implementation of a blockchain arrangement suitable for use with the system of embodiments of the invention;

[084] Figure 16 is a block diagram in accordance with yet a further preferred embodiment of the present invention and;

[085] Figure 17 is a detailed block diagram of the system of figure 10C and figure 16;

Description of Embodiments

[086] It should be noted in the following description that like or the same reference numerals in different embodiments denote the same or similar features.

System 100 of computing devices

[087] Fig. 1 shows a system 100 of computing devices adapted for implementation of various embodiments of the present invention.

[088] As such, the system 100 comprises a first digital device 110 and a second digital device 114 connected to a network 116. According to various embodiments, the first digital device 110 is one of, but not limited to, a mobile phone, a desktop computer, a laptop or a tablet etc. Similarly, according to various embodiments, the second digital device is one of, but not limited to, a mobile phone, a desktop computer, a laptop or a tablet etc. Further, the network 116 is one of, but not limited to, a Wide Area Network (WAN) or a Local Area

Network (LAN). Preferably the network 116 is internet. The first digital device 110 and the second digital device 114 are also able to communicate through a second network 112. In one embodiment of the invention, the second network 112 is a telecommunication network such as internet or a mobile telecommunication network. In another embodiment, the second network 112 is a non-telecommunication network such as Bluetooth and Near Field Communication (NFC) etc.

[089] Further, the system 100 comprises a first intermediary server 126 and a second intermediary server 128 connected to the network 116. In one embodiment of the invention, the first intermediary server 126 and the second intermediary server 128 represent a first financial institution and a second financial institution, respectively. In one embodiment of the invention, the respective first and second financial institutions are different branches of different of different banks. In another embodiment, the respective first and second financial institutions are different branches of a single bank. In various other embodiments, the respective first and second financial institutions are, but not limited to, commercial banks, investment banks, brokerages, investment companies etc. It is to be noted that each one of the first intermediary server 126 and the second intermediary server 128 may represent a system of servers comprising web servers, application servers, database servers and gateway servers.

[090] Further, the first intermediary server 126 is operably connected to a first document store 132 and the second intermediary server 128 is operably connected to the second document store 134. In one embodiment, the first document store 132 and the second document store 134 represent databases configured to store a plurality of documents. Each one of the documents comprise data pertaining to a financial transaction and metadata corresponding to the data. In various embodiments, metadata comprises format, encoding, author, hash, verification and relationships to other documents.

[091] Further, the system 100 comprises a financial messaging server 130 connected to the network 116. The financial messaging server 130 provides a financial messaging service between any two intermediary servers, including the

first intermediary server 126 and the second intermediary server 128. Some of the examples of financial messaging services include SWIFT (Society for Worldwide Interbank Financial Telecommunication) for cross border transactions. ACH (Automated Clearing House) used in USA and RTGS (Real Time Gross Settlement) used in India and Hong Kong.

[092] Further, the system 100 comprises a token server 120 connected to the network 116 and a token database 122. Further, a blockchain 124 is connected to the network 116. Further, a messaging bus 118 is connected to the network 116. The messaging bus 118 represents a messaging server or a system of messaging servers configured to enable a plurality of applications/servers/devices to communicate with each other. In one embodiment, the messaging bus 118 also comprises an authentication/ authorization server for authorizing the computing devices communicating through the messaging bus 118. The detailed configuration of the messaging bus 118 has been described in the discussion to follow.

[093] Also, a blockchain 124 is connected to the network 116. The configuration and/or the functioning of the first intermediary server 126, the second intermediary server 128, the first document store 132, the second document store 134, the token server 120, the token database 122, the blockchain 124, and the messaging bus 118 has been described below in a description. The system 100 for processing a financial transaction involves subsystems of the computing devices, which have been depicted by means of figures and description as following. The description below has been explained with embodiments comprising a financial transaction between a first user and a second user. In some embodiments, the first user acts as a biller/ beneficiary/payee and the second user acts as purchaser/payer. In other embodiments, the first user acts as a payer and the second user acts as a payee/beneficiary. Further, it is to be noted that the first user and the second user may represent any number of entities involved in the financial transaction.

[094] In one embodiment of the invention, the first user may instruct the first intermediary sever 126 to process the financial transaction. In one embodiment, the financial transaction involves generation of an invoice for the second user

and receiving a payment from the second user, by the first user. In another embodiment, the financial transaction involves making the payment to the second user, by the first user. Specifically, the first user connects with the first intermediary server 126 through the network 116, using the first digital device 110.

[095] Figure 2 illustrates a subsystem (200) of the computing devices for generation of a token, in accordance with a preferred embodiment of the present invention. As shown in figure 2, the first digital device 110 comprises a first processor 210 operably connected to a first memory 220. The first memory 220 comprises a first computer program code, the first computer program code when executed by the first processor 210 instructs the first processor 210 to instruct the first intermediary server 126 to process the financial transaction. Further, in one embodiment of the invention, the first computer program code further instructs the first processor 210 to provide one or more documents pertaining to the financial transaction, to the first intermediary server 126. In another embodiment, the one or more documents are already available with the first intermediary server 126. In yet another embodiment, the first intermediary server 126 is configured to generate at least one document from the one or more documents.

[096] The at least one document may be, but is not limited to, a request for processing the financial transaction. The first intermediary server 126 is configured to transmit the one or more documents pertaining to the financial transaction, to the first document store 132. In one embodiment of the invention, the one or more documents comprise payment metadata such as, but is not limited to, account numbers of the first user (or a beneficiary), Business Identifier Codes (BIC) of the financial institutions corresponding to the first intermediary server 126 and the second intermediary server 128, amount of currency to be transferred and type of currency etc.

[097] Further, in accordance with an embodiment, the one or more documents comprise one or more first regulatory compliance documents pertaining to the first user. Some examples of the regulatory compliance documents include, but are not limited to purpose of payment documents, a result of sanctions screening

and secondary identifiers such as date of birth proof, address proof or other Know Your Customer (KYC) documents.

[098] The first intermediary server 126 is further configured to generate an enriched data record from the one or more documents and add the enriched data record into the blockchain 124. The first intermediary server 126 is configured to generate the enriched data record in multiple ways in multiple embodiments, some of the embodiments have been elucidated below.

[099] In one embodiment of the invention, the first intermediary server 126 is configured to extract a plurality of attributes from the one or more documents. The plurality of attributes may comprise, but are not limited to, originator attributes, beneficiary attributes and purpose of payment etc. Further, the first intermediary server 126 is configured to combine the plurality of attributes to generate the enriched data record. In another embodiment of the present invention, the first intermediary server 126 is configured to extract the plurality of attributes from one or more documents, de-identify the plurality of attributes to obtain a plurality of de-identified attributes and combine the plurality of de-identified attributes to generate the enriched data record. In yet another embodiment of the present invention, the first intermediary server 126 is configured to extract the plurality of attributes from the one or more documents, hash the plurality of attributes to generate a plurality of respective hashes and combine the plurality of hashes to generate the enriched data record.

[0100] Further, the blockchain 124 is a data structure comprising a plurality of blocks of data. Each block of data from the plurality of blocks of data represents a single financial transaction. Further, the blockchain 124 is configured to store data pertaining to the financial transaction in association with the token. The data pertaining to the financial transaction includes, but is not limited to, the enriched data record, a plurality of hashes, a plurality of public keys etc. Also the blockchain 124 is configured to return the data pertaining to the financial transaction, when queried using the token.

[0101] Further, the first intermediary server 126 is configured to request generation of a token, to the token server 120, via the messaging bus 118. The token server

120 in turn is configured to generate the token and add the token into the blockchain 124. The token is stored in the blockchain 124, in association with the enriched data record. Further, the token server 120 is configured to transmit the token to the first intermediary server 126, via the messaging bus 118. Further, the first intermediary server 126 is configured to transmit the token to the first document store 132. The token is stored in the first document store 132, in association with the one or more documents.

[0102] In one embodiment of the invention, the token server 120 is further configured to implement a smart contract and add the smart contract into the blockchain 124. In one embodiment, the smart contract is a shared, signed and verifiable program code which is distributed and/or executed on the blockchain 124. The smart contract would run on the blockchain 124 and would be stored in association with the token.

[0103] In one embodiment of the invention, before proceeding any further, the first intermediary server 126 may wish to perform certain "checks", by communicating with the second intermediary server 128, via the messaging bus 118. For enabling communication, the first intermediary server 126 is configured to generate a first asymmetrical pair of a first public key and a first private key. Further, the first intermediary server 126 is configured to add the first public key and a first address of the first intermediary server 126 into the blockchain 124. Similarly, the second intermediary server 128 is configured to generate a second asymmetrical pair of a second public key and a second private key. Further, the second intermediary server 128 is configured to add the second public key and a second address of the second intermediary server 128 into the blockchain 124.

[0104] Fig. 3 illustrates a subsystem (300) of the computing devices for exchange of requests and responses between the first intermediary server 126 and the second intermediary server 128, via the messaging bus118, in accordance with a preferred embodiment of the present invention. During communication with the second intermediary server 128, the first intermediary server 126 is configured to transmit one or more first requests, each comprising the token, to the second intermediary server 128, via the messaging bus 118. Examples of one or more first requests comprise, but are not limited to, KYC check and payment

acceptance. In one embodiment of the invention, the the one or more first requests are transmitted on basis of a plurality of predefined criterion. For example, if the first intermediary server 126 is required to make the payment to the second intermediary server 128, the first intermediary server 126 may necessitate KYC check of the second user. The second intermediary server 128 is configured to then receive the one or more first requests from the first intermediary server 126 and transmit the one or more first requests and the token to the second document store 134. In one embodiment of the invention, the one or more first requests are transmitted to the second documents store 134 in form of one or more first request documents.

[0105] Further, the second intermediary server 128 is configured to generate one or more first responses, each comprising the token, corresponding to the respective one or more first requests. In one embodiment of the invention, the one or more first responses are generated in form of one or more first response documents at the second intermediary server 128. Further, the second intermediary server 128 is configured to transmit the one or more first responses to the first intermediary server 126, via the messaging bus 118. As an extension of the example above, the second intermediary server 128 may then send a validation successful response to the first intermediary server 126, via the messaging bus 118. In one embodiment of the invention, the one or more first responses comprise one or more second regulatory compliance documents pertaining to a second user.

[0106] Further, the second intermediary server 128 is configured to hash the one or more first requests and the one or more first responses to generate one or more first request hashes and one or more first response hashes, respectively. Also, the second intermediary server 128 is configured to add the one or more first request hashes and the one or more first response hashes to the enriched data record in the blockchain 124. The first intermediary server 126 is then configured to receive the one or more first responses and transmit the one or more first responses to the first document store 132. In one embodiment of the invention, the first intermediary server 126 is further configured to hash the one or more first responses to regenerate the one or more first response hashes. Further, the first intermediary server 126 is configured to verify the one or more first response hashes with the blockchain 124, using the token. The first intermediary server

126 can ensure that the one or more first responses are same as the ones generated at the second intermediary server 128.

[0107] In one embodiment of the invention, to enable secure transmission, the first intermediary server 126 is configured to encrypt each one of the one or more first requests with the second public key and sign each one of the one or more first requests with the first public key, before transmission to the second intermediary server 128. Consequently, the second intermediary server 128 is configured to decrypt the each one of the one or more first requests with the second private key after reception from the first intermediary server 126. In a similar manner, the second intermediary server 128 is configured to encrypt each one of the one or more first responses with the first public key and sign the each one of the one or more first responses with the second public key, before transmission to the first intermediary server 126. Consequently, the first intermediary server 126 is configured to decrypt each one of the one or more first responses with the first private key after reception from the second intermediary server 128.

[0108] The second intermediary server 128 may also request certain compliance checks. Therefore, the second intermediary server 128 is further configured to transmit one or more second requests, each comprising the token, to the first intermediary server 126, via the messaging bus 118. Examples of the one or more second requests comprise, but are not limited to, sender sanctions screening check. The first intermediary server 126 is in turn configured to receive the one or more second requests and transmit the one or more second requests to the first document store 132. In one embodiment of the invention, the one or more second requests are transmitted to the first document store 132 in form of one or more second request documents. Further the first intermediary server 126 is configured to generate one or more second responses, each comprising the token, corresponding to the respective one or more second requests. In one embodiment of the invention, the one or more second responses are generated in form of one or more second response documents. Further, the first intermediary server 126 is configured to transmit the one or more second responses to the second intermediary server 128, via the messaging bus 118. In one embodiment of the invention, the one or more second responses comprise

the one or more first regulatory compliance documents pertaining to the first user.

[0109] Further, the first intermediary server 126 is configured to hash the one or more second requests and the one or more second responses to generate one or more second request hashes and one or more second response hashes, respectively. Further, the first intermediary server 126 is configured to add the one or more second request hashes and the one or more second response hashes to the enriched data record in the blockchain 124. The second intermediary server 128 is in turn configured to receive the one or more second responses and transmit the one or more second responses to the second document store 134. In one embodiment of the invention, the second intermediary server 128 is further configured to hash the one or more second responses to regenerate the one or more second response hashes and verify the one or more second response hashes with the blockchain 124, using the token. Thus ensuring that the one or more second responses are same as those generated at the first intermediary server 126.

[0110] In one embodiment of the invention, to enable secure communication, the second intermediary server 128 is configured to encrypt each one of the one or more second requests with the first public key and sign each one of the one or more second requests with the second public key, before transmission to the first intermediary server 126. Consequently, the first intermediary server 126 is configured to decrypt the each one of the one or more second requests with the first private key after reception from the second intermediary server 128. In a similar manner, the first intermediary server 126 is configured to encrypt each one of the one or more second responses with the second public key and sign the each one of the one or more second responses with the first public key, before transmission to the second intermediary server 128. Consequently, the second intermediary server 128 is configured to decrypt the each one of the one or more second responses with the second private key after reception from the first intermediary server 126.

[0111] The requests and the responses are transmitted in a secure manner across the messaging bus 118, in form of a plurality of messages. It is to be noted that

each one of the plurality of messages comprises a content hash of all its contents to ensure that the contents have not been altered during transmission. The request and/or receipt time of the recipient public key are also attached to the plurality of messages. This ensures only recipient can see message contents & ensures revocability of public keys.

[0112] In one embodiment of the invention, the first intermediary server 128 is further configured to assign a payment risk rating to the token. In one embodiment of the invention, the payment risk rating is assigned to the token at the first intermediary server 126 after completion of the communication with the second intermediary server 128. The payment risk rating provides a pointer to the regulatory and other compliance checks performed by the first intermediary server 126 and the second intermediary server 128. In one embodiment of the invention, the first intermediary server 126 is further configured to add the payment risk rating to the enriched data record in the blockchain 124. Further, the blockchain 124 is configured to return the payment risk rating when queried with the token. The payment risk rating enables better straight through processing by reducing exceptions and false positives.

[0113] The token thus generated may be used to make the payment to the second user by the first user or making the payment to the first user, by the second user. Figure 4 illustrates a subsystem (400) of the computing devices for making the payment to the second user, by the first user. As shown in the figure 4, the first intermediary server 126 is configured to send a first financial message comprising the token, to the second intermediary server 128, indicative of making the payment to the second user. The first financial message is sent through the financial messaging server 130.

[0114] Figure 5 illustrates a subsystem (500) of computing devices for making the payment to the first user, by the second user. As shown in the figure 5, the first intermediary server 126 is further configured to transmit the token to the first digital device 110. In turn, the first computer program code instructs the first processor 210 to receive the token from the first intermediary server 126. In one embodiment of the invention, the first processor 210 is further instructed to provide the token to the second digital device 114 via the network 116 or the

second network 112. The second digital device 110 comprises a second memory 520 and a second processor 510 operably connected to the second memory 520, the second memory 520 comprising a second computer program code, the second computer program code when executed by the second processor 510, instructs the second processor 510 to receive the token from the first digital device 110 and provide the token to the second intermediary server 128.

[0115] In turn the second intermediary server 128 is configured to receive the token from the second digital device 114, transmit the token to the second document store 134 and send a second financial message comprising the token, to the first intermediary server 126, indicative of making the payment to the first user. Further, the second financial message is sent through the financial messaging server 130.

Computing device

[0116] Fig. 56 shows a computing device 600. In a preferred embodiment, the computing device 600 takes the form of the first intermediary server 126, the second intermediary server 128, the token server 120 and the financial messaging server 190 as described above. In this manner, the computing device 500 is adapted to comprise functionality for communication with the network 116, storage capability (such as the token database 122) for storing a plurality of tokens and respective creators of the plurality of tokens.

[0117] However, it should be noted that each one first digital device 110 and the second digital device 114, as shown in figure 1, may also be depicted as the computing device 600. In this manner, the computing device may comprise differing technical integers, such as the display device 6020, one or more human interface devices 660 and the like. In other words, the technical integers of the computing device 500 is shown in figure 5 are exemplary only and variations, adaptations and the like may be made thereto within the purposive scope of the embodiments described herein and having regard for the particular application of the computing device 600.

[0118] In particular the steps of the computer implemented method for processing of a financial transaction, as described in further detail below, may be implemented as computer program code instructions executable by the computing device 600. The computer program code instructions may be divided into one or more computer program code instruction libraries, such as dynamic link libraries (DLL), wherein each of the libraries performs a one or more steps of the computer implemented method. Additionally, a subset of the one or more of the libraries may perform graphical user interface tasks relating to the steps of the computer implemented method.

[0119] The device 600 comprises semiconductor memory 610 comprising volatile memory such as random access memory (RAM) or read only memory (ROM). The memory 600 may comprise either RAM or ROM or a combination of RAM and ROM.

[0120] The device 600 comprises a computer program code storage medium reader 630 for reading the computer program code instructions from computer program code storage media 620. The storage media 620 may be optical media such as CD-ROM disks, magnetic media such as floppy disks and tape cassettes or flash media such as USB memory sticks.

[0121] The device further comprises I/O interface 640 for communicating with one or more peripheral devices. The I/O interface 640 may offer both serial and parallel interface connectivity. For example, the I/O interface 640 may comprise a Small Computer System Interface (SCSI), Universal Serial Bus (USB) or similar I/O interface for interfacing with the storage medium reader 630. The I/O interface 640 may also communicate with the one or more human interface devices (HID) 660 such as keyboards, pointing devices, joysticks and the like. The I/O interface 640 may also comprise a computer to computer interface, such as a Recommended Standard 232 (RS-232) interface, for interfacing the device 600 with one or more personal computer (PC) devices 690. The I/O interface 640 may also comprise an audio interface for communicate audio signals to one or more audio devices 6050, such as a speaker or a buzzer.

[0122] The device 600 also comprises a network interface 650 for communicating with one or more computer networks 680. The network 680 may be a wired network, such as a wired Ethernet™ network or a wireless network, such as a Bluetooth™ network or IEEE 802.11 network. The network 680 may be a local area network (LAN), such as a home or office computer network, or a wide area network (WAN), such as the Internet or private WAN.

[0123] The device 600 comprises an arithmetic logic unit or processor 6000 for performing the computer program code instructions. The processor 6000 may be a reduced instruction set computer (RISC) or complex instruction set computer (CISC) processor or the like. The device 600 further comprises a storage device 6030, such as a magnetic disk hard drive or a solid state disk drive.

[0124] Computer program code instructions may be loaded into the storage device 6030 from the storage media 620 using the storage medium reader 630 or from the network 680 using network interface 650. During the bootstrap phase, an operating system and one or more software applications are loaded from the storage device 6030 into the memory 610. During the fetch-decode-execute cycle, the processor 6000 fetches computer program code instructions from memory 610, decodes the instructions into machine code, executes the instructions and stores one or more intermediate results in memory 600.

[0125] In this manner, the instructions stored in the memory 610, when retrieved and executed by the processor 6000, may configure the computing device 600 as a special-purpose machine that may perform the functions described herein.

[0126] The device 600 also comprises a video interface 6010 for conveying video signals to a display device 6020, such as a liquid crystal display (LCD), cathode-ray tube (CRT) or similar display device.

[0127] The device 600 also comprises a communication bus subsystem 665 for interconnecting the various devices described above. The bus subsystem 665 may offer parallel connectivity such as Industry Standard Architecture (ISA), conventional Peripheral Component Interconnect (PCI) and the like or serial

connectivity such as PCI Express (PCIe), Serial Advanced Technology Attachment (Serial ATA) and the like.

Embodiments of the method

[0128] Figure 7 illustrates a computer implemented method 700 for processing a financial transaction in accordance with an embodiment of the present invention. As described above, the financial transaction is assumed to be taking place between the first user and the second user. The method begins at step 710 by transmitting the one or more documents pertaining to the financial transaction, from the first intermediary server 126 to the first document store 132. In one embodiment of the invention, the one or more documents are provided to the first intermediary server 126 by the first user, from the first digital device 110. In another embodiment, the one or more documents are already available with the first intermediary server 126. In yet another embodiment, the at least one document from the one or more documents is generated at the first intermediary server 126.

[0129] At step 720, the enriched data record is generated from the one or more documents, at the first intermediary server 126. Further, the enriched data record is added into the blockchain 124, from the first intermediary server 126. The enriched data record may be generated in different manners in different embodiments. Some of the embodiments have been discussed below.

[0130] In one embodiment of the invention, the plurality of attributes are extracted from the one or more documents, at the first intermediary server 126. Further, the plurality of attributes are combined to generate the enriched data record at the first intermediary server 126.

[0131] In another embodiment, the plurality of attributes are extracted from the one or more documents, at the first intermediary server 126. Further, the plurality of attributes are de-identified to obtain the plurality of de-identified attributes at the first intermediary server 126. The de-identification of the plurality of attributes comprises removal of any information from the plurality of attributes which may link the plurality of attributes to the first user or the second user. This is to ensure

the confidentiality of the first user and the second user, in case the enriched data record is accessed through illegal routes. The plurality of de-identified attributes are then combined, at the first intermediary server 126, to generate the enriched data record.

[0132] In yet another embodiment, the plurality of attributes are extracted from the one or more documents, at the first intermediary server 126. Further, the plurality of attributes are hashed to generate the plurality of respective hashes, at the first intermediary server 126. The plurality of hashes are then combined to generate the enriched data record, at the first intermediary server 126.

[0133] At step 730, the token server 120 is requested to generate the token corresponding to the financial transaction, from the first intermediary server 126, via the messaging bus 118. At step 740, the token is generated at the token server 120. Further, the token is added into the blockchain 124, from the token server 120. At step 750, the token is transmitted from the token server 120 to the first intermediary server 126. At step 760, the token is transmitted from the first intermediary server 126 to the first document store 132. Further, the token is stored in association with the one or more documents, in the first document store 132.

[0134] In one embodiment of the invention, the smart contract is implemented at the token server 120. Further, the smart contract is added into the blockchain, from the token server 120.

[0135] In one embodiment of the invention, the first intermediary server 126 communicates with the second intermediary server 128, via the messaging bus 118. The communication may take place for verification and validation of the first user and the second user. In one embodiment of the invention, the first asymmetrical pair of the first public key and the first private key is generated at the first intermediary server 126. Further, the first public key and the first address of the first intermediary server 126 are added into the blockchain 124, from the first intermediary server 126. Similarly, the second asymmetrical pair of the second public key and the second private key is generated at the second intermediary server. Further, the second public key and the second address of

the second intermediary server 128 are added into the blockchain 124, from the second intermediary server 128.

[0136] In one embodiment, during communication, the one or more first requests, each comprising the token, are transmitted from the first intermediary server 126 to the second intermediary server 128, via the messaging bus 118. Further, the one or more first requests are received at the second intermediary server 128 and the one or more first requests and the token are transmitted from the second intermediary server 128 to a second document store 134. Further, one or more first responses, each comprising the token, corresponding to the respective one or more first requests, are generated at the second intermediary server 128. Further, the one or more first responses are transmitted from the second intermediary server 128 to the first intermediary server 126, via the messaging bus 118. Further, the one or more first requests and the one or more first responses are hashed at the second intermediary server 128 to generate one or more first request hashes and one or more first response hashes, respectively. Further, the one or more first request hashes and the one or more first response hashes are added to the enriched data record in the blockchain 124, from the second intermediary server 128. Also, the one or more first responses are received at the first intermediary server 126 and transmitted to the first document store 132.

[0137] In one embodiment of the invention, the one or more first responses comprise the one or more second regulatory compliance documents pertaining to the second user. Further, in one embodiment of the invention, the one or more first responses are hashed at the first intermediary server 126 to regenerate the one or more first response hashes. Also, the one or more first response hashes are verified with the blockchain 124 from the first intermediary server 126, using the token.

[0138] In one embodiment of the invention, for secure communication, each one of the one or more first requests are encrypted with the second public key and signed with the first public key at the first intermediary server 126, before transmission to the second intermediary server 128. Consequently, the each one of the one or more first requests are decrypted with the second private key at the

second intermediary server 128 after reception from the first intermediary server 126. Similarly, each one of the one or more first responses are encrypted with the first public key and signed with the second public key at the second intermediary server 128, before transmission to the first intermediary server 126. Also, consequently, the each one of the one or more first responses are decrypted with the first private key at the first intermediary server 126 after reception from the second intermediary server 128.

[0139] Similarly, in the present and various other embodiments, during communication, the one or more second requests, each comprising the token, are transmitted from the second intermediary server 128 to the first intermediary server 126, via the messaging bus 118. Further, the one or more second requests are received at the first intermediary server 126 and the one or more second requests are transmitted from the first intermediary server 126 to the first document store 132. Further, one or more second responses, each comprising the token, corresponding to the respective one or more second requests, are generated at the first intermediary server 126. Further, the one or more second responses are transmitted from the first intermediary server 126 to the second intermediary server 128, via the messaging bus 118. Further, the one or more second requests and the one or more second responses are hashed at the first intermediary server 126 to generate one or more second request hashes and one or more second response hashes, respectively. Further, the one or more second request hashes and the one or more second response hashes are added to the enriched data record in the blockchain 124, from the first intermediary server 126. Also, the one or more second responses are received at the second intermediary server 128 and transmitted to the second document store 134.

[0140] In one embodiment of the invention, the one or more second responses comprise the one or more first regulatory compliance documents pertaining to the first user. Further, in one embodiment, the one or more second responses are hashed at the second intermediary server 128 to regenerate the one or more second response hashes. Also, the one or more second response hashes are verified with the blockchain 124 from the second intermediary server 128, using the token.

[0141] In one embodiment of the invention, for secure communication, each one of the one or more second requests are encrypted with the first public key and signed with the second public key at the second intermediary server 128, before transmission to the first intermediary server 126. Consequently, the each one of the one or more second requests are decrypted with the first private key at the first intermediary server 126 after reception from the second intermediary server 128. Similarly, each one of the one or more second responses are encrypted with the second public key and signed with the first public key at the first intermediary server 126, before transmission to the second intermediary server 128, and decrypted with the second private key at the second intermediary server 128 after reception from the first intermediary server 126.

[0142] In one embodiment of the invention, the payment risk rating is assigned to the token, at the first intermediary server 126. Further, the payment risk rating is added to the enriched data record in the blockchain 124, from the first intermediary server 126.

[0143] In one embodiment, for making the payment to second user, by the first user, the first financial message comprising the token, is sent from the first intermediary server 126 to the second intermediary server 128, indicative of making the payment to the second user. Further, the first financial message is sent via the financial messaging server 130.

[0144] In another embodiment, the token is transmitted from the first intermediary server 126 to the first digital device 110, available with the first user. The first processor 210 receives the token from the first intermediary server 126 and stores the token in the first memory 220. Further, the token is provided to the second user, by the first user. In one embodiment, the token is provided to the second user by means of a Quick Response (QR) code printed on an invoice. In another embodiment, the token is provided to the second user at the second digital device 114 available with the second user, from the first digital device 110. The second processor 510 receives the token from the first digital device 110, and stores the token in the second memory 520.

[0145] Further, the token is provided to the second intermediary server 128, from the second digital device 114, by the second user. The second computer program code instructs the second processor 510 to provide the token to the second intermediary server. The token is then transmitted to the second document store 134, from the second intermediary server 128. Further, the second financial message is sent from the second intermediary server 128, to the first intermediary server 126, indicative of making the payment to the first user.

Prior Art

[0146] With reference to Figure 8A there is illustrated in block form the basic components of a prior art settlement system. In many transactions there will be an at least first transacting entity 811 which enters into a financial transaction with an at least second transacting entity 812. The financial transaction may be as simple as the agreement by the first transacting entity 811 to sell a particular item or service to the second transacting entity 812. Typically the financial transaction will require settlement for an agreed amount expressed in a Fiat or other currency. In the vast majority of cases the at least first transacting entity 811 will be associated with an at least first intermediary entity 813, in this instance in the form of a bank A and similarly the second transacting entity 812 will be associated with an at least second intermediary entity 814 in this instance in the form of bank B. The first transacting entity 811 will have a first bank account 815 at the first intermediary entity 813 whilst second transacting entity 812 will have a second bank account 816 at second intermediary entity 814. Settlement of any given transaction requires instruction given by first transacting entity 811 to its first intermediary entity 813 to pay an agreed amount from the first bank account 815 to the bank account comprising second bank account 816 of second intermediary entity 814 of second transacting entity 812. For these instructions to be carried out metadata in the form of payment metadata 817 must be assembled at the first intermediary entity 813 sufficient and exhaustive to communicate to the second intermediary entity 814 such that the agreed settlement amount is transmitted from bank A to bank B and more particularly to the specific accounts of the respective first transacting entity 811 and second transacting entity 812.

[0147] A similar transaction may be applied in reverse where the second transacting entity sells a good or service to first transacting entity 811. In such an instance the respective intermediaries, once having received the respective payment metadata 817 and exchanged that metadata 817 may elect to simply pay the difference 818 electronically as between the intermediaries to effect the multiple transactions. In some instances, particularly where the financial transaction is cross-border-for example the first intermediary entity 813 is in a first country whilst the second intermediary entity 814 is in a second country the metadata 817 may include what is known as a Swift code which is a substantially unique identifier for each intermediary entity involved in the financial transaction. However, for any given transaction, far more data than merely a unique identifier for each intermediary entity involved in a financial transaction is required in order for the appropriate settlement amounts to ultimately be recorded in the correct accounts and settle the financial transaction for the agreed amounts.

[0148] Figure 8B is a data and funds flow diagram of data and funds flow according to a prior art settlement system at the granular level. In this instance, with reference to figure 8B like components are numbered as for figure 8A a given transaction requiring settlement can be embodied as a bill 890 which will include payment data 891 and may include bank facilitation payment data 892 comprising, in this instance, a biller code and a financial transaction code. Banks which are party to this bank facilitation payment system permit data entry by entity B (or payer B) 812 into a database of bank B 814 by means of a bank application or web interface 814 B. Bank B may then add additional data to form metadata 817 which is sent to a third-party server 893 which utilises metadata 817 to trigger pay (settlement) of bill 890 from payer B bank 814 to biller A bank 813.

Exemplary Embodiments

[0149] With reference to Figure 9C there is illustrated a block diagram of the basic infrastructure and components suited for use with embodiments of the present invention. In this instance like components are numbered as for figure 8 except in the 900 series. So, for example, first transacting entity 811 becomes first transacting entity 911 in this embodiment with reference to figure 2C

[0150] In this instance a settlement system 910 according to a generalised embodiment includes at least first transacting entity 911 which enters into a financial transaction with at least a second transacting entity 912. As previously these entities are associated with a respective first intermediary entity 913 and a second intermediary entity 914 in the form of bank A and bank B. Each of the first transacting entity 911 and a second transacting entity 912 has a respective account 915, 916 at their respective intermediary entities as illustrated in figure 9C

[0151] In this instance, in the event that first transacting entity 911 enters into a financial transaction with second transacting entity 912 then, at the time of entry into the financial transaction 920, a token 921 is generated. In this instance the token 921 is generated by at least first digital device 922 communicating with a token database 923. The token database 923 generates a token comprising a data file 924 containing all data that will ultimately be required to settle the financial transaction 920 including any necessary identifying information for the transacting entity is, their accounts and the intermediary entities. Settlement is effected by communication of the token 921 to bank A and then to bank B together with the appropriate flow of funds.

[0152] With reference to figure 9A at the granular level a bill 990 from a biller 911 directed to a payer 912 contains bill data 991 and also token data of a token 921 residing within a code symbol 994 (in this instance a QR code). The token data includes pointer data pointing to data 995 on token database 923. The data 995 combined with bank ID data 914 permits the creation by token database 923 of a full payment record 996 which can be utilised to cause settlement of the bill 990 as against payer 912 via, in this instance, their respective banks 914, 913.

[0153] With reference to figure 9B the payment data record 996 is utilised has fed into a settlement network such as, for example a network 997 operating under the Ripple protocol thereby permitting substantially real-time settlement across multiple institutions and banks.

[0154] With reference to Figures 10 there is illustrated in block diagram form a first preferred embodiment of the present invention by way of a non-limiting example of a financial transaction. In this embodiment like components are numbered as for the previous embodiments except in the 1000 series. So, for example, token 921 becomes token 1021.

[0155] With reference to figure 10A the financial transaction system 1010 is activated, as for the previous embodiment, when a financial transaction 1020 is entered into between at least first transacting entity 1011 and at least a second transacting entity 1012 each dealing, for the purposes of this transaction, through respective intermediary entities 1013, 1014.

[0156] At the time of and as part of entry into the financial transaction 1020 the first transacting entity 1011 accesses token database 1023 via digital device 1022 executing via a web browser interface or via execution of an application running on a portable digital devices such as a mobile telephone or in a further alternative as a point-of-sale terminal in order to arrange for the database 1023 to generate a token 1021. In this instance the token 1021 will include better data 1024 including the recipient named, BIC, IBAN, destination country, mobile number, currency, business type, communication, payment amount. In this instance the token 1021 including the metadata 1024 is stored in the token database 1023. In addition the first transacting entity 1011 communicates the token 1021 to a digital device 1030 associated with second transacting entity 1012. In this instance the communication is by way of initial transmission of the token 1021 to digital device 1022 which then on transmits the token via Internet 1031 to digital device 1030.

[0157] With reference to figure 10B, when ready to settle the financial transaction 1020 the second transacting entity 1012 "logs in" to a portal associated with second intermediary entity 1014 and communicates the token 1021. In this instance have the login can be executed via a web browser associated with digital device 1030 which communicates via Internet 1031 the token 1021 to a digital processing system 1032 (including at least a processor and a memory) associated with second intermediary entity 1014. Substantially at the same time as part of seeking to settle the financial transaction 1020:

[0158] Notification: token database 1023 notifies second intermediary entity 1014 to contact the token database 1023 from which it receives a further token 1021A.

[0159] Verification: token database 1023 communicates with the processing system 1032 of second intermediary entity 1014 to verify that sufficient funds are located in account 1016 as indicated in the meta data 1024 to settle the financial transaction.

[0160] Committing payer funds: payers bank debits payers account: payers bank sends notice to payer bank gateway: payers bank gateway calls token database 1023 to get approved token:

[0161] Settlement: gateway of payers bank sends by way of non-limiting example XRP (the native currency of the Ripple protocol) to billers bank gateway: payers bank gateway notifies token database 1023 of receipt:

[0162] Clearing: payer's bank Nostro account is debited subject to bank institution rules.

[0163] Examples of tokenised messages and their generation and transmission are illustrated in pseudocode below. Reference to "sparro" is a reference to an instance of a token databasep23.

[0164] The previous, meta-data mode is first. It switches to minimal half way through

[0165] --

[0166] Bank:HSBC >> createUserCode >> Sparro:Sparro

[0167] {"id":"User:ABC Paper","name":"ABC Paper"}

[0168] (Creating Sparro User Code - Meta-data given can be used by other banks for compliance and for confirming payee with customers.)

[0169] --

[0170] Bank:MayBank >> createUserCode >> Sparro:Sparro

[0171] {"id":"User:XYZ Printing","name":"XYZ Printing"}

[0172] (Creating Sparro User Code - Meta-data given can be used by other banks for compliance and for confirming payee with customers.)

[0173] --

[0174] Sparro:Sparro >> createUserCode-reply >> Bank:HSBC

[0175] {"id":"User:ABC Paper","name":"ABC Paper","code":"65q3gdd"}

[0176] --

[0177] Sparro:Sparro >> createUserCode-reply >> Bank:MayBank

[0178] {"id":"User:XYZ Printing","name":"XYZ Printing","code":"70wqgx6"}

[0179] --

[0180] User:ABC Paper >> createInvoice >> Bank:HSBC

[0181] {"amount":{"amount":1000,"currency":"gbp"}}

[0182] --

[0183] Bank:HSBC >> createInvoiceCode >> Sparro:Sparro

[0184] {"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd"}

[0185] (Creating Invoice Code - An invoice code is created by Sparro and connected to the bank.)

[0186] -

[0187] Sparro:Sparro >> createInvoiceCode-reply >> Bank:HSBC

[0188] {"code":"6tq6wcbad"}

[0189] --

[0190] Bank:HSBC >> createInvoice-reply >> User:ABC Paper

[0191]
{"invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

[0192] Abc invoice { amount: { amount: 1000, currency: 'gbp' },

[0193] payee: '65q3gdd',

[0194] code: '6tq6wcbad' }

[0195] --

[0196] User:ABC Paper >> invoice >> User:XYZ Printing

[0197]
{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}

[0198] -

[0199] User:XYZ Printing >> payInvoice >> Bank:MayBank

[0200] {"invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300}}

[0201] --

[0202] Bank:MayBank >> sendMoney >> BankGateway:MayBank

[0203]

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300}}

[0204] --

[0205] BankGateway:MayBank >> getInvoice >> Sparro:Sparro

[0206] "6tq6wcbad"

[0207] (Sending Payment to Invoice - The payment is sent to the bank that created the invoice.)

[0208] --

[0209] Sparro:Sparro >> getInvoice-reply >> BankGateway:MayBank

[0210]

{"bank":"Bank:HSBC","invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

[0211] --

[0212] BankGateway:MayBank >> transfer >> BankGateway:HSBC

[0213]

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":"ripple-1"}

[0214] --

[0215] BankGateway:HSBC >> incomingTransfer >> Bank:HSBC

[0216]

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":"ripple-1"}

[0217] --

[0218] BankGateway:HSBC >> transfer-reply >> BankGateway:MayBank

[0219] {"success":true,"owed":{"GBP":300}}

[0220] --

[0221] Bank:HSBC >> getInvoice >> Sparro:Sparro

[0222] "6tq6wcbad"

[0223] --

[0224] BankGateway:MayBank >> sendMoney-reply >> Bank:MayBank

[0225]

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":"ripple-1"}

[0226] --

[0227] Sparro:Sparro >> getInvoice-reply >> Bank:HSBC

[0228]

{"bank":"Bank:HSBC","invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

[0229] --

[0230] Bank:MayBank >> payInvoice-reply >> User:XYZ Printing

[0231]

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":"ripple-1"}

[0232] XYZ part-paid invoice {

[0233] "payer": "70wqgx6",

[0234] "invoice": "6tq6wcbad",

[0235] "amount": {

[0236] "currency": "GBP",

[0237] "amount": 300

[0238] },

[0239] "id": "ripple-1"

[0240] }

[0241] --

[0242] Bank:HSBC >> incomingTransfer >> User:ABC Paper

[0243]

{"invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"},"transfer":{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":"ripple-1"}}

[0244] -

[0245] User:XYZ Printing >> payInvoice >> Bank:MayBank

[0246] {"invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700}}

[0247] --

[0248] Bank:MayBank >> sendMoney >> BankGateway:MayBank

[0249]

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700}}

[0250] --

[0251] BankGateway:MayBank >> getInvoice >> Sparro:Sparro

[0252] "6tq6wcbad"

[0253] (Sending Payment to Invoice - The payment is sent to the bank that created the invoice.)

[0254] --

[0255] Sparro:Sparro >> getInvoice-reply >> BankGateway:MayBank

[0256]

{"bank":"Bank:HSBC","invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

[0257] --

[0258] BankGateway:MayBank >> transfer >> BankGateway:HSBC

[0259]

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700},"id":"ripple-2"}

[0260] --

[0261] BankGateway:HSBC >> incomingTransfer >> Bank:HSBC

[0262]

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700},"id":"ripple-2"}

[0263] --

[0264] BankGateway:HSBC >> transfer-reply >> BankGateway:MayBank

[0265] {"success":true,"owed":{"GBP":1000}}

[0266] --

[0267] Bank:HSBC >> getInvoice >> Sparro:Sparro

[0268] "6tq6wcbad"

[0269] -

[0270] BankGateway:MayBank >> sendMoney-reply >> Bank:MayBank

[0271]

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700},"id":"ripple-2"}

[0272] --

[0273] Sparro:Sparro >> getInvoice-reply >> Bank:HSBC

[0274]

{"bank":"Bank:HSBC","invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

[0275] --

[0276] Bank:MayBank >> payInvoice-reply >> User:XYZ Printing

[0277]

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700},"id":"ripple-2"}

[0278] XYZ finished paying invoice {

[0279] "payer": "70wqgx6",

[0280] "invoice": "6tq6wcbad",

[0281] "amount": {

[0282] "currency": "GBP",

[0283] "amount": 700

[0284] },

[0285] "id": "ripple-2"

[0286] }

[0287] --- SWITCHING TO MODE: minimal ---

[0288] --

[0289] Bank:HSBC >> incomingTransfer >> User:ABC Paper

[0290]

{"invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"},"transfer":{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700},"id":"ripple-2"}}

[0291] --Bank:HSBC >> createUserCode >> Sparro:Sparro

[0292] undefined

[0293] (Creating Sparro User Code - No meta-data is required.)

[0294] --

[0295] Bank:MayBank >> createUserCode >> Sparro:Sparro

[0296] undefined

[0297] (Creating Sparro User Code - No meta-data is required.)

[0298] --

[0299] Sparro:Sparro >> createUserCode-reply >> Bank:HSBC

[0300] {"code":"dnt7gec"}

[0301] --

[0302] Sparro:Sparro >> createUserCode-reply >> Bank:MayBank

[0303] {"code":"6wwpwuc"}

[0304] --

[0305] User:ABC Paper >> createInvoice >> Bank:HSBC

[0306] {"amount":{"amount":2000,"currency":"gbp"}}

[0307] --

[0308] Bank:HSBC >> createInvoiceCode >> Sparro:Sparro

[0309] null

[0310] (Creating Invoice Code - An invoice code is created by Sparro and connected to the bank. No invoice details are required.)

[0311] --

[0312] Sparro:Sparro >> createInvoiceCode-reply >> Bank:HSBC

[0313] {"code":"erwkax1md"}

[0314] --Bank:HSBC >> createInvoice-reply >> User:ABC Paper

[0315]

{"invoice":{"amount":{"amount":2000,"currency":"gbp"},"code":"erwkax1md","payee":"User:ABC Paper","transfers":[]}}

[0316] Abc invoice { amount: { amount: 2000, currency: 'gbp' },

[0317] code: 'erwkax1md',

[0318] payee: 'User:ABC Paper',

[0319] transfers: [] }

[0320] --

[0321] User:ABC Paper >> invoice >> User:XYZ Printing

[0322]

{"amount":{"amount":2000,"currency":"gbp"},"code":"erwkax1md","payee":"User:ABC Paper","transfers":[]}

[0323] --

[0324] User:XYZ Printing >> payInvoice >> Bank:MayBank

[0325] {"invoice":"erwkax1md","amount":{"currency":"GBP","amount":600}}

[0326] --

[0327] Bank:MayBank >> sendMoney >> BankGateway:MayBank

[0328]

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600}}

[0329] --

[0330] BankGateway:MayBank >> getInvoice >> Sparro:Sparro

[0331] "erwkax1md"

[0332] (Sending Payment to Invoice - The payment is sent to the bank that created the invoice.)

[0333] --

[0334] Sparro:Sparro >> getInvoice-reply >> BankGateway:MayBank

[0335] {"bank":"Bank:HSBC"}

[0336] --

[0337] BankGateway:MayBank >> transfer >> BankGateway:HSBC

[0338]

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}

[0339] --

[0340] BankGateway:HSBC >> incomingTransfer >> Bank:HSBC

[0341]

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}

[0342] --

[0343] BankGateway:HSBC >> transfer-reply >> BankGateway:MayBank

[0344] {"success":true,"owed":{"GBP":600}}

[0345] --

[0346] Bank:HSBC >> incomingTransfer >> User:ABC Paper

[0347]

{"invoice":{"amount":{"amount":2000,"currency":"gbp"},"code":"erwkax1md","payee":"User:ABC Paper","transfers":[{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}]},"transfer":{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}}

[0348] --

[0349] BankGateway:MayBank >> sendMoney-reply >> Bank:MayBank

[0350]

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}

[0351] --

[0352] Bank:MayBank >> payInvoice-reply >> User:XYZ Printing

[0353]

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}

[0354]

[0355] XYZ part-paid invoice {

[0356] "payer": "6wwpwuc",

[0357] "invoice": "erwkax1md",

[0358] "amount": {

[0359] "currency": "GBP",

[0360] "amount": 600

[0361] },

[0362] "id": "ripple-3"

[0363] }

[0364] --

[0365] User:XYZ Printing >> payInvoice >> Bank:MayBank

[0366] {"invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400}}

[0367] --

[0368] Bank:MayBank >> sendMoney >> BankGateway:MayBank

[0369]

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400}}

[0370] --

[0371] BankGateway:MayBank >> getInvoice >> Sparro:Sparro

[0372] "erwkax1md"

[0373] (Sending Payment to Invoice - The payment is sent to the bank that created the invoice.)

[0374] --

[0375] Sparro:Sparro >> getInvoice-reply >> BankGateway:MayBank

[0376] {"bank":"Bank:HSBC"}

[0377] -

[0378] BankGateway:MayBank >> transfer >> BankGateway:HSBC

[0379]

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}

[0380] --

[0381] BankGateway:HSBC >> incomingTransfer >> Bank:HSBC

[0382]

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}

[0383] BankGateway:HSBC >> transfer-reply >> BankGateway:MayBank

[0384] {"success":true,"owed":{"GBP":2000}}

[0385] --

[0386] Bank:HSBC >> incomingTransfer >> User:ABC Paper

[0387]

{"invoice":{"amount":{"amount":2000,"currency":"gbp"},"code":"erwkax1md","payee":"User:ABC Paper","transfers":[{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"},{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}]},"transfer":{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}}

[0388] --

[0389] BankGateway:MayBank >> sendMoney-reply >> Bank:MayBank

[0390]

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}

[0391] --

[0392] Bank:MayBank >> payInvoice-reply >> User:XYZ Printing

[0393]

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}

[0394] XYZ finished paying invoice {

[0395] "payer": "6wwpwuc",

[0396] "invoice": "erwkax1md",

[0397] "amount": {

[0398] "currency": "GBP",

[0399] "amount": 1400

[0400] },

[0401] "id": "ripple-4"

[0402] }

[0403] features of this embodiment include the enablement of a private, invitation only, network for banking institutions which, in a particular form, can facilitate cross-border payments thereby to enable substantially real-time payments at reduced processing cost.

[0404] With reference to figure 11 there is shown a block diagram of salient characteristics of a messaging system 810 of the prior art as compared with the salient messaging characteristics of the system 1010 enabled by the code listed above and more broadly described with reference to the earlier embodiments.

[0405] Figure 12 illustrates the options for data content to be included in tokens in accordance with embodiments of the invention as described above.

[0406] Figure 13 provides a comparison of characteristics of embodiments of the present invention as compared with the prior art Swift-based messaging system at a commercial layer 1270, a security layer 1271 and a technical layer 1272

[0407] Embodiments of the invention can be implemented utilising the "Ripple" the framework, protocol and gateway-or more generally any blockchain based framework. In a particular form the final settlement process can be enabled through a Ripple frame work thereby to facilitate substantially real-time settlement across multiple institutions and multiple banks.

[0408] Figure 14 is a block diagram of a further embodiment. In this instance a distributed ledger 1381 operating on blockchain principles provides for transmission of the tokenised message as for previous embodiments.

[0409] In this instance it will be observed that the tokenised transmission distributed ledger 1381 operates in parallel with conventional transmission between institution A and institution B.

[0410] Conventional transmission includes transmission of conventional messages utilising the SWIFT protocol. It is also to be noted that institution A and institution B may be subsidiaries of the same institution or may otherwise be closely related. In the alternative they may be completely independent institutions.

[0411] The tokenised message as described in previous embodiments may include information as typically transmitted by the SWIFT or other current acknowledged data transmission systems for transmission of financial information for the purpose of transfer of funds between parties.

[0412] The tokenised message may transmit data which includes some of the data normally included in the conventional message. In alternative forms it may include additional data. In yet alternative forms it may include data not transferred at all in the data normally included in the conventional message.

[0413] The aim, in particular forms, ultimately, is to improve the reliability of the financial transaction as between the first transacting entity and the second transacting entity and, in some forms, to provide an enhanced capability.

[0414] In the arrangement of figure 14 the data comprising the tokenised message is transmitted via nodes 1380 within a blockchain 1381.

[0415] In summary, Bank A and Bank B might be branches of the same bank, say HSBC HK and HSBC China (which today use SWIFT for intrabank transfers). So this system could be used within 1 financial institution.

[0416] In one form the purpose of storing the token only in the blockchain is really to both de-identify the information in the blockchain (which is critical for banks), and enable use of existing (SWIFT / ACH / RTGS) or new messaging systems to send the payment instruction in tokenised format. Banks today have significant investment in existing conventional messaging systems and a complete abandonment of these messaging systems would not be feasible. However settlement is still a manual process so linking the conventional messaging system to the 'blockchain' settlement system (via the token) is an important feature of this embodiment. So, in diagram 7 we include a SWIFT/ACH/RTGS connection between the two Financial Institutions (FIs) (or branches) for communication of the token, and the blockchain ledger is common. The data that is required to settle the payment can be provided by the FI's customer or by the FI themselves (say from a core banking system or similar).

[0417] Fig 15 illustrates in block diagram form key components of an implementation of a blockchain structure which may be utilised to implement the system of figure 14.

[0418] Each block includes verified transactions and the blockchain maintains a ledger all prior transactions. The blockchain is duplicated by all the computers on a network.

[0419] The first block in the chain is known as the Genesis block and new blocks can be added in linear and chronological order. From any given block in the

chain the information of this genesis block and all blocks that led back to this one can be retrieved. A blockchain is essentially numerous blocks connected through hash chaining where each block is comprised of the following (see figure 15):

[0420] Timestamp: provides proof that the data in a block existed at a particular time;

[0421] Previous Hash: Essentially a pointer to the previous block;

[0422] Merkle Hash: Summary of all executed transactions;

[0423] Nonce: Individual blocks identity and is an arbitrary number which can only be used once.

[0424] The blockchain is managed by a network of distributed nodes where each node contains a copy of the entire blockchain. Each node in the network can add blocks to the chain, where every node is adding blocks at the same point in the chain at the same time. The more nodes that comprise the network the harder it is to disrupt the storage of the blockchain. Unlike centralised systems which rely on a single authority, there is no single point of failure in these distributed nodes network. If you change the content of a block you change its Hash.

[0425] Blockchains can be based on/ operate in association with any one of a number of protocols – for example Ripple or Stellar.

[0426] Figure 15B shows a first step in creation of records in the block chain structure of figure 15A whilst figure 15C shows a second step in the creation of records in the chain structure of figure 15A. The chain structures of this type may be utilised in relation to the embodiments described in this application.

[0427] Figure 16 is a block diagram of a further embodiment wherein the parallel data transmission capabilities of the system are further detailed as compared with the embodiment of figure 14 .Components are numbered as for previous embodiments except in the 1400 series. So, for example, first transacting entity 1311 of the further embodiment of figure 14 becomes the first transacting entity 1411. In this instance a distributed ledger 1481 operating on blockchain principles (refer description with reference to figure 15) provides for transmission of the tokenised message as for previous embodiments.

[0428] In this instance it will be observed that the tokenised transmission distributed ledger 1481 operates in parallel with conventional transmission between institution A and institution B.

[0429] Conventional transmission includes transmission of conventional messages utilising the SWIFT protocol. It is also to be noted that institution A 1413 and institution B 1414 may be subsidiaries of the same institution or may otherwise be closely related. In the alternative they may be completely independent institutions.

[0430] The tokenised message 1490 as described in previous embodiments may include information as typically transmitted by the SWIFT or other current acknowledged data transmission systems for transmission of financial information for the purpose of transfer of funds between parties.

[0431] The tokenised message may transmit data which includes some of the data normally included in the conventional message. In alternative forms and more particularly the form with reference to figure 16 it may include additional data however, in this instance the additional data 1491 is transmitted via blockchain 881 as an entry in a shared ledger 1492. The additional data 1491 in this instance comprises a token value 1493, a financial transaction value 1494 a sender cheque status flag 895 and a token state 1496. This entry 1497 in shared ledger 1492 can be accessed based on token value 1493. In an alternative form the entry 1497 and more particularly the token value 1493 may be secured for example requiring a separate key before the data can be accessed and/or decrypted. The data in entry 1497 may comprise deidentified data thereby to ensure that no personally identifiable information is transmitted to Bank (second intermediary entity 1414).

[0432] The aim, ultimately, is to improve the reliability of the financial transaction as between the first transacting entity and the second transacting entity and, in some forms, to provide an enhanced capability.

[0433] In particular, in preferred forms an element includes provision of systems which add additional information whereby the additional information is to enrich payments with more information given the inability of existing payment systems to communicate enriched information.

[0434] In the arrangement of figure 16 the data comprising the tokenised message is transmitted via nodes 1480 within a blockchain 1481.

[0435] In summary, Bank A and Bank B might be branches of the same bank, say HSBC HK and HSBC China (which today use SWIFT for intrabank transfers). So this system could be used within 1 financial institution.

[0436] In one form the purpose of storing the token only in the blockchain is really to both de-identify the information in the blockchain (which is critical for banks), and enable use of existing (SWIFT / ACH / RTGS) or new messaging systems to send the payment instruction in tokenised format. Banks today have significant investment in existing conventional messaging systems and a complete abandonment of these messaging systems would not be feasible. However settlement is still a manual process so linking the conventional messaging system to the 'blockchain' settlement system (via the token) is an important feature of this embodiment. So, in figure 16 we include a SWIFT/ACH/RTGS connection between the two Financial Institutions (FIs) (or branches) for communication of the token, and the blockchain ledger is common. The data that is required to settle the payment can be provided by the FI's customer or by the FI themselves (say from a core banking system or similar).

[0437] Figure 17 is a detailed block diagram of the system of figure 10C and figure 16.

[0438] With reference to Figure 17 there is illustrated in block diagram form a first preferred embodiment of the present invention by way of a non-limiting example of a financial transaction. In this embodiment like components are numbered as for Figure 16 in the 1400 series.

[0439] With reference to figure 17 the financial transaction system 1010 is activated, as for the previous embodiment, when a financial transaction 1020 is entered into between at least first transacting entity 1011 and at least a second transacting entity 1012 each dealing, for the purposes of this transaction, through respective intermediary entities 1013, 1014.

[0440] At the time of and as part of entry into the financial transaction 1020 the first transacting entity 1011 accesses token database 1023 via digital device 1022 executing via a web browser interface or via execution of an application running on a portable digital devices such as a mobile telephone or in a further alternative as a point-of-sale terminal in order to arrange for the database 1023 to generate a token 1021. In this instance the token 1021 will include better data 1024 including the recipient named, BIC, IBAN, destination country, mobile number, currency, business type, communication, payment amount. In this instance the token 1021 including the metadata 1024 is stored in the token database 1023. In addition the first transacting entity 1011 communicates the token 1021 to a digital device 1030 associated with second transacting entity 1012. In this instance the communication is by way of initial transmission of the token 1021 to digital device 1022 which then on transmits the token via Internet 1031 to digital device 1030.

[0441] With reference to figure 17, when ready to settle the financial transaction 1020 the second transacting entity 1012 "logs in" to a portal associated with second intermediary entity 1014 and communicates the token 1021. In this instance have the login can be executed via a web browser associated with digital device 1030 which communicates via Internet 1031 the token 1021 to a digital processing system 1032 (including at least a processor and a memory) associated with second intermediary entity 1014. Substantially at the same time as part of seeking to settle the financial transaction 1020:

[0442] Notification: token database 1023 notifies second intermediary entity 1014 to contact the token database 1023 from which it receives a further token 1021A.

[0443] Verification: token database 1023 communicates with the processing system 1032 of second intermediary entity 1014 to verify that sufficient funds are located

in account 1016 as indicated in the meta data 1024 to settle the financial transaction.

[0444] Committing payer funds: payers bank debits payers account: payers bank sends notice to payer bank gateway: payers bank gateway calls token database 1023 to get approved token:

[0445] Settlement: gateway of payers bank sends by way of non-limiting example XRP (the native currency of the Ripple protocol) to billers bank gateway: payers bank gateway notifies token database 1023 of receipt:

[0446] Clearing: payer's bank may be a Nostro account which is debited subject to bank institution rules.

[0447] Embodiments of the invention can be implemented utilising the "Ripple" framework, protocol and gateway-or more generally any blockchain based framework. In a particular form the final settlement process can be enabled through a Ripple framework thereby to facilitate substantially real-time settlement across multiple institutions and multiple banks.

[0448] With further reference to figure 17 it will be observed that the token 1021, in this instance, may be conveyed between bank 1013 and bank 1014 by way of a medium 1060 utilizing the SWIFT protocol or other compatible protocols 1050. In preferred forms the medium the medium will be an electronic communications medium and in particular forms may be implemented by way of a VPN established between bank 1013 and bank 1014.

[0449] Separately deidentified data 1051 A, B, C, D associated with the financial transaction to which the token pertains may be transmitted over a separate communication medium, in this instance internet 1031. In a preferred form the communication medium utilizes a blockchain structure as described earlier in this specification and the deidentified data 1051 A, B, C, D is located within a record structure 1061 which is replicated throughout the blockchain structure.

[0450] In use a sellers bank 1013 as part of entering into the financial transaction with buyers bank 1014 will establish a SWIFT transaction transmittable over medium 1060. Separately and preferably in parallel the sellers bank 1013 will perform associated operations needed to complete the financial transaction such as verification of the buyers ID and related characteristics. Data related to these associated operations is then placed in record structure 1061 and that record is placed into the blockchain structure. The associated data includes deidentifed data 1051 A, B, C, D.

[0451] This data is available to the buyers bank 1014 by way of the buyers bank logging into the blockchain structure and receiving the deidentified data which is associated with the financial transaction which is represented by token 1021. Thereby allowing assembly by the buyers bank 1014 of all necessary data to execute the financial transaction on behalf of the buyer and seller.

[0452] With reference to figures 16 and 17 the system provides for communication of invoice/purchase order /remittance advice information as illustrated.

[0453] It will be further observed that blockchain structures may be utilized to provide an information layer above existing legacy systems (for example based on SWIFT protocols and the like) and wherein the additional information layer provides enriched information about payments using the token. It is to be noted that existing systems do not provide enriched information and, in more particular forms, do not provide deidentified information/data for use by the communicating parties.

[0454] The above describes only some embodiments of the present invention and modifications, obvious to those skilled in the art, can be made thereto without departing from the scope of the present invention.

[0455] The computer implemented method and the system for processing a financial transaction offers a plurality of advantages. First, the invention enables a wide variety of documents to be attached to a financial transaction, by means of a token. The existing financial messaging systems allow only specific information to be attached to the financial transaction. Further, the invention enables

generation of an auditable enriched data record from the documents. The enriched data record is stored in a distributed ledger (or the blockchain) and can be retrieved at any time when queried with the token. Further, the enriched data record ensures that integrity of the documents is maintained in perpetuity. Further, the documents stores enable maintaining of a state of the token. That is, a status of the financial transaction can be tracked at any time, from the respective documents stored in the document stores.

Other Exemplary Embodiments

[0456] Definitions:

[0457] Token: in this specification a "token" is a pointer to an enriched data record of a plurality data required to process a financial transaction and wherein the plurality of data is rendered, formatted or passed through an algorithm in a predetermined manner. The process of rendering, formatting or passing through an algorithm in a predetermined manner is termed "tokenisation". The tokenisation process may involve operations such as encryption and de-identification of the plurality of data.

[0458] Financial Transaction: in this specification "financial transaction" refers to a trade between two parties, for example at least a first transacting entity and a second transacting entity and wherein the trade is expressed in a financial form (for example in a Fiat currency or an electronic currency-to be distinguished, for example, from a barter transaction) which will ultimately require exchange of currency to process the financial transaction. In some instances the currency will be the same on both sides of the financial transaction. In other cases a conversion from one currency to another may be required.

[0459] Personally Identifiable Information (PII): in this specification refers to information that a regulator or privacy policy will not allow to be disclosed to a third party.

[0460] Accordingly, in one broad form of the invention, there is provided a system for settling a financial transaction electronically; said system comprising:

at least a first transacting entity;

at least a second transacting entity;

at least a first intermediary entity;

at least a second intermediary entity;

in the case where the first transacting entity enters into a financial transaction with the second transacting entity generating a tokenised message at the time of the financial transaction containing data needed to settle the financial transaction;

initiating settlement of the financial transaction by transmission of the tokenised message to the at least first transacting entity.

[0461] In a further broad form of the invention there is provided a tokenised message construction system; said system comprising:

a server in communication with a database and which facilitates communications between a plurality of parties to a financial transaction;

each party having a digitised device with which to communicate with other ones of the parties and with the server;

each party capable of generating a tokenised message via a bidirectional communication with the server.

[0462] Accordingly, in yet a further broad form of the invention there is provided tokenised message construction system; said system comprising:

a server in communication with a database and which facilitates communications between a plurality of parties to a financial transaction;

each party having a digitised device with which to communicate with other ones the parties and with the server;

each party capable of generating a tokenised message via a bidirectional communication with the server.

[0463] Preferably the tokenised message is generated with reference to a token database located at a remote location.

[0464] Preferably the tokenised message includes at least a first data element, a second data element and a third data element.

[0465] Preferably the first data element comprises identification data for a payor, the second data element comprises identification data for a payee (biller) and the third data element comprises identification currency, denomination and value data.

[0466] Preferably a further tokenised message is generated by either an intermediary entity or the token database.

[0467] Preferably a tokenised message is generated by a bi-directional communication process.

[0468] Preferably the bi-directional communication process is between the token database and an intermediary entity.

[0469] Preferably a step in producing a tokenised message involves de-identifying data.

[0470] Preferably a step in producing a tokenised message involves adding a data element to the message.

[0471] Preferably a step in producing a tokenised message involves removing a data element from the message.

[0472] Preferably a step in producing a tokenised message involves applying an algorithm to the data elements in the message.

[0473] Preferably the token database sequences the tokenised messages.

[0474] Preferably the token database sequences the tokenised messages and transmits the tokenised messages as payment data records to a blockchain settlement system.

[0475] Preferably the blockchain settlement system employs the Ripple protocol.

[0476] Preferably the tokenised message includes at least a first data element, a second data element and a third data element.

[0477] Preferably the first data element comprises identification data for a payor, the second data element comprises identification data for a payee (biller) and the third data element comprises identification currency, denomination and value data.

[0478] Preferably a further tokenised message is generated by either an intermediary entity or the token database.

[0479] Preferably a tokenised message is generated by a bi-directional communication process.

[0480] Preferably the bi-directional communication process is between the token database and an intermediary entity.

[0481] Preferably a step in producing a tokenised message involves de-identifying data.

[0482] Preferably a step in producing a tokenised message involves adding a data element to the message.

[0483] Preferably a step in producing a tokenised message involves removing a data element from the message.

[0484] Preferably a step in producing a tokenised message involves applying an algorithm to the data elements in the message.

[0485] Preferably the token database sequences the tokenised messages.

[0486] Preferably the token database sequences the tokenised messages and transmits the tokenised messages as payment data records to a blockchain settlement system.

[0487] Preferably the blockchain settlement system employs the Ripple protocol.

[0488] Preferably a second message is transmitted between the intermediaries.

[0489] Preferably the second message is tokenised.

[0490] Preferably the second message contains conventional data.

[0491] Preferably the second message is transmitted by means of a blockchain system.

[0492] Preferably the second message includes information equivalent to that transmitted by the SWIFT system.

[0493] Preferably the tokenised message includes additional information beyond that transmitted by the SWIFT system.

[0494] The system wherein the tokenised message includes information which verifies the security status of at least one party to the financial transaction.

[0495] Preferably the second tokenised message includes information which verifies the security status of both parties to the financial transaction.

[0496] Preferably the token is conveyed by way of a medium utilizing the SWIFT messaging system or other compatible messaging system.

[0497] Preferably the medium is implemented by way of a VPN.

[0498] Preferably deidentified data associated with the financial transaction to which the token pertains is transmitted over a separate communication medium.

[0499] Preferably the separate communication medium utilizes a blockchain structure.

[0500] Preferably the deidentified data is located within a record structure which is replicated throughout the blockchain structure.

[0501] Preferably in use a sellers bank as part of entering into the financial transaction with buyers bank will establish a SWIFT transaction.

[0502] Preferably in parallel the sellers bank will perform associated operations needed to complete the financial transaction such as verification of the buyers ID and related characteristics.

[0503] Preferably data related to the associated operations is then placed in a record structure and that record is placed into the blockchain structure.

[0504] Preferably the associated data includes deidentifed data.

[0505] Preferably the data is available to the buyers bank by way of the buyers bank logging into the blockchain structure and receiving the deidentified data which is associated with the financial transaction which is represented by the token thereby allowing assembly by the buyers bank of all necessary data to execute the financial transaction on behalf of the buyer and seller.

[0506] Preferably incorporating secure channels thereby permitting only selected entities to communicate the data to execute the financial transaction on behalf of the buyer and seller.

Advantages

[0507] The invention is not limited to interaction between two banks only, but can be extended to any number of banks involved in the financial transaction. For example, the token can be included in all the financial messages sent between a plurality of banks, and the token can be used by any bank from the plurality of banks to verify the financial transaction from the enriched data record, before taking any further steps in the process.

[0508] The messaging bus allows all the financial institutions involved in the financial transaction to communicate in real-time and ensure that the payer, the

beneficiary, and all the parameters corresponding to the financial transaction are validated. Further, encryption/decryption of the requests and responses using asymmetrical pairs of keys ensures that the transmission of the request and the responses is always secure. Further, the payment risk rating ensures better straight through processing by reducing exceptions and false positives. Also, the token is compatible with a large array of formats, including JSON, XML, CSV, SWIFT, over a number of transports, including HTTP, FTP, AMQP, and JMS.

Interpretation

[0509] Unless otherwise defined, all terms (including technical and scientific terms) used herein have the same meaning as commonly understood by one of ordinary skill in the art to which this invention belongs. It will be further understood that terms used herein should be interpreted as having a meaning that is consistent with their meaning in the context of this specification and the relevant art and will not be interpreted in an idealized or overly formal sense unless expressly so defined herein. For the purposes of the present invention, additional terms are defined below. Furthermore, all definitions, as defined and used herein, should be understood to control over dictionary definitions, definitions in documents incorporated by reference, and/or ordinary meanings of the defined terms unless there is doubt as to the meaning of a particular term, in which case the common dictionary definition and/or common usage of the term will prevail.

[0510] The terminology used herein is for the purpose of describing particular embodiments only and is not intended to be limiting of the invention. As used herein, the singular articles "a", "an" and "the" are intended to include the plural forms as well, unless the context clearly indicates otherwise and thus are used herein to refer to one or to more than one (i.e. to "at least one") of the grammatical object of the article. By way of example, the phrase "an element" refers to one element or more than one element.

[0511] The term "about" is used herein to refer to quantities that vary by as much as 30%, preferably by as much as 20%, and more preferably by as much as 10% to a reference quantity. The use of the word 'about' to qualify a number is merely an express indication that the number is not to be construed as a precise value.

[0512] Throughout this specification, unless the context requires otherwise, the words "comprise", "comprises" and "comprising" will be understood to imply the inclusion of a stated step or element or group of steps or elements but not the exclusion of any other step or element or group of steps or elements.

[0513] The term "real-time" for example "displaying real-time data," refers to the display of the data without intentional delay, given the processing limitations of the system and the time required to accurately measure the data.

[0514] As used herein, the term "exemplary" is used in the sense of providing examples, as opposed to indicating quality. That is, an "exemplary embodiment" is an embodiment provided as an example, as opposed to necessarily being an embodiment of exemplary quality for example serving as a desirable model or representing the best of its kind.

[0515] The phrase "and/or," as used herein in the specification and in the claims, should be understood to mean "either or both" of the elements so conjoined, i.e., elements that are conjunctively present in some cases and disjunctively present in other cases. Multiple elements listed with "and/or" should be construed in the same fashion, i.e., "one or more" of the elements so conjoined. Other elements may optionally be present other than the elements specifically identified by the "and/or" clause, whether related or unrelated to those elements specifically identified. Thus, as a non-limiting example, a reference to "A and/or B", when used in conjunction with open-ended language such as "comprising" can refer, In one embodiment of the invention, to A only (optionally including elements other than B); in another embodiment, to B only (optionally including elements other than A); in yet another embodiment, to both A and B (optionally including other elements); etc.

[0516] As used herein in the specification and in the claims, "or" should be understood to have the same meaning as "and/or" as defined above. For example, when separating items in a list, "or" or "and/or" shall be interpreted as being inclusive, i.e., the inclusion of at least one, but also including more than one, of a number or list of elements, and, optionally, additional unlisted items. Only terms clearly indicated to the contrary, such as "only one of" or "exactly one

of," or, when used in the claims, "consisting of" will refer to the inclusion of exactly one element of a number or list of elements. In general, the term "or" as used herein shall only be interpreted as indicating exclusive alternatives (i.e. "one or the other but not both") when preceded by terms of exclusivity, such as "either," "one of," "only one of," or "exactly one of." "Consisting essentially of," when used in the claims, shall have its ordinary meaning as used in the field of patent law.

[0517] As used herein in the specification and in the claims, the phrase "at least one," in reference to a list of one or more elements, should be understood to mean at least one element selected from any one or more of the elements in the list of elements, but not necessarily including at least one of each and every element specifically listed within the list of elements and not excluding any combinations of elements in the list of elements. This definition also allows that elements may optionally be present other than the elements specifically identified within the list of elements to which the phrase "at least one" refers, whether related or unrelated to those elements specifically identified. Thus, as a non-limiting example, "at least one of A and B" (or, equivalently, "at least one of A or B," or, equivalently "at least one of A and/or B") can refer, In one embodiment of the invention, to at least one, optionally including more than one, A, with no B present (and optionally including elements other than B); in another embodiment, to at least one, optionally including more than one, B, with no A present (and optionally including elements other than A); in yet another embodiment, to at least one, optionally including more than one, A, and at least one, optionally including more than one, B (and optionally including other elements); etc.

Bus

[0518] In the context of this document, the term "bus" and its derivatives, while being described in a preferred embodiment as being a communication bus subsystem for interconnecting various devices including by way of parallel connectivity such as Industry Standard Architecture (ISA), conventional Peripheral Component Interconnect (PCI) and the like or serial connectivity such as PCI Express (PCIe), Serial Advanced Technology Attachment (Serial ATA) and the like, should be construed broadly herein as any system for communicating data.

In accordance with:

[0519] As described herein, 'in accordance with' may also mean 'as a function of' and is not necessarily limited to the integers specified in relation thereto.

Composite items

[0520] As described herein, 'a computer implemented method' should not necessarily be inferred as being performed by a single computing device such that the steps of the computer implemented method may be performed by more than one cooperating computing devices.

[0521] Similarly objects as used herein such as 'web server', 'server', 'client computing device', 'computer readable medium' and the like should not necessarily be construed as being a single object, and may be implemented as a two or more objects in cooperation, such as, for example, a web server being construed as two or more web servers in a server farm cooperating to achieve a desired goal or a computer readable medium being distributed in a composite manner, such as program code being provided on a compact disk activatable by a license key downloadable from a computer network.

Database:

[0522] In the context of this document, the term "database" and its derivatives may be used to describe a single database, a set of databases, a system of databases or the like. The system of databases may comprise a set of databases wherein the set of databases may be stored on a single implementation or span across multiple implementations. The term "database" is also not limited to refer to a certain database format rather may refer to any database format. For example, database formats may include MySQL, MySQLi , XML or the like.

Wireless:

[0523] The invention may be embodied using devices conforming to other network standards and for other applications, including, for example other WLAN standards and other wireless standards. Applications that can be accommodated include IEEE 802.11 wireless LANs and links, and wireless Ethernet.

[0524] In the context of this document, the term "wireless" and its derivatives may be used to describe circuits, devices, systems, methods, techniques, communications channels, etc., that may communicate data through the use of modulated electromagnetic radiation through a non-solid medium. The term does not imply that the associated devices do not contain any wires, although in some embodiments they might not. In the context of this document, the term "wired" and its derivatives may be used to describe circuits, devices, systems, methods, techniques, communications channels, etc., that may communicate data through the use of modulated electromagnetic radiation through a solid medium. The term does not imply that the associated devices are coupled by electrically conductive wires.

Processes:

[0525] Unless specifically stated otherwise, as apparent from the following discussions, it is appreciated that throughout the specification discussions utilizing terms such as "processing", "computing", "calculating", "determining", "analysing" or the like, refer to the action and/or processes of a computer or computing system, or similar electronic computing device, that manipulate and/or transform data represented as physical, such as electronic, quantities into other data similarly represented as physical quantities.

Processor:

[0526] In a similar manner, the term "processor" may refer to any device or portion of a device that processes electronic data, e.g., from registers and/or memory to transform that electronic data into other electronic data that, e.g., may be stored in registers and/or memory. A "computer" or a "computing device" or a "computing machine" or a "computing platform" may include one or more processors.

[0527] The computer implemented methodologies described herein are, in one embodiment of the invention, performable by one or more processors that accept computer-readable (also called machine-readable) code containing a set of instructions that when executed by one or more of the processors carry out at least one of the computer implemented methods described herein. Any processor capable of executing a set of instructions (sequential or otherwise) that specify actions to be taken are included. Thus, one example is a typical

processing system that includes one or more processors. The processing system further may include a memory subsystem including main RAM and/or a static RAM, and/or ROM.

Computer-Readable Medium:

[0528] Furthermore, a computer-readable carrier medium may form, or be included in a computer program product. A computer program product can be stored on a computer usable carrier medium, the computer program product comprising a computer readable program means for causing a processor to perform a method as described herein.

Networked or Multiple Processors:

[0529] In alternative embodiments, the one or more processors operate as a standalone device or may be connected, e.g., networked to other processor(s), in a networked deployment, the one or more processors may operate in the capacity of a server or a client machine in server-client network environment, or as a peer machine in a peer-to-peer or distributed network environment. The one or more processors may form a web appliance, a network router, switch or bridge, or any machine capable of executing a set of instructions (sequential or otherwise) that specify actions to be taken by that machine.

[0530] Note that while some diagram(s) only show(s) a single processor and a single memory that carries the computer-readable code, those in the art will understand that many of the components described above are included, but not explicitly shown or described in order not to obscure the inventive aspect. For example, while only a single machine is illustrated, the term "machine" shall also be taken to include any collection of machines that individually or jointly execute a set (or multiple sets) of instructions to perform any one or more of the computer implemented methodologies discussed herein.

Additional Embodiments:

[0531] Thus, one embodiment of each of the computer implemented methods described herein is in the form of a computer-readable carrier medium carrying a set of instructions, e.g., a computer program that are for execution on one or more processors. Thus, as will be appreciated by those skilled in the art, embodiments of the present invention may be embodied as a method, an

apparatus such as a special purpose apparatus, an apparatus such as a data processing system, or a computer-readable carrier medium. The computer-readable carrier medium carries computer readable code including a set of instructions that when executed on one or more processors cause a processor or processors to implement a method. Accordingly, aspects of the present invention may take the form of a method, an entirely hardware embodiment, an entirely software embodiment or an embodiment combining software and hardware aspects. Furthermore, the present invention may take the form of carrier medium (e.g., a computer program product on a computer-readable storage medium) carrying computer-readable program code embodied in the medium.

Carrier Medium:

[0532] The software may further be transmitted or received over a network via a network interface device. While the carrier medium is shown in an example embodiment to be a single medium, the term "carrier medium" should be taken to include a single medium or multiple media (e.g., a centralized or distributed database, and/or associated caches and servers) that store the one or more sets of instructions. The term "carrier medium" shall also be taken to include any medium that is capable of storing, encoding or carrying a set of instructions for execution by one or more of the processors and that cause the one or more processors to perform any one or more of the computer implemented methodologies of the present invention. A carrier medium may take many forms, including but not limited to, non-volatile media, volatile media, and transmission media.

Implementation:

[0533] It will be understood that the steps of methods discussed are performed In one embodiment of the invention by an appropriate processor (or processors) of a processing (i.e., computer) system executing instructions (computer-readable code) stored in storage. It will also be understood that the invention is not limited to any particular implementation or programming technique and that the invention may be implemented using any appropriate techniques for implementing the functionality described herein. The invention is not limited to any particular programming language or operating system.

Means For Carrying out a Method or Function

[0534] Furthermore, some of the embodiments are described herein as a method or combination of elements of a method that can be implemented by a processor of a processor device, computer system, or by other means of carrying out the function. Thus, a processor with the necessary instructions for carrying out such a method or element of a method forms a means for carrying out the computer implemented method or element of a method. Furthermore, an element described herein of an apparatus embodiment is an example of a means for carrying out the function performed by the element for the purpose of carrying out the invention.

Connected

[0535] Similarly, it is to be noticed that the term connected, when used in the claims, should not be interpreted as being limitative to direct connections only. Thus, the scope of the expression a device A connected to a device B should not be limited to devices or systems wherein an output of device A is directly connected to an input of device B. It means that there exists a path between an output of A and an input of B which may be a path including other devices or means. "Connected" may mean that two or more elements are either in direct physical or electrical contact, or that two or more elements are not in direct contact with each other but yet still co-operate or interact with each other.

Embodiments:

[0536] Reference throughout this specification to "one embodiment" or "an embodiment" means that a particular feature, structure or characteristic described in connection with the embodiment is included in at least one embodiment of the present invention. Thus, appearances of the phrases "In one embodiment of the invention" or "in an embodiment" in various places throughout this specification are not necessarily all referring to the same embodiment, but may. Furthermore, the particular features, structures or characteristics may be combined in any suitable manner, as would be apparent to one of ordinary skill in the art from this disclosure, in one or more embodiments.

[0537] Similarly it should be appreciated that in the above description of example embodiments of the invention, various features of the invention are sometimes grouped together in a single embodiment, figure, or description thereof for the

purpose of streamlining the disclosure and aiding in the understanding of one or more of the various inventive aspects. This method of disclosure, however, is not to be interpreted as reflecting an intention that the claimed invention requires more features than are expressly recited in each claim. Rather, as the following claims reflect, inventive aspects lie in less than all features of a single foregoing disclosed embodiment. Thus, the claims following the Detailed Description of Specific Embodiments are hereby expressly incorporated into this Detailed Description of Specific Embodiments, with each claim standing on its own as a separate embodiment of this invention.

[0538] Furthermore, while some embodiments described herein include some but not other features included in other embodiments, combinations of features of different embodiments are meant to be within the scope of the invention, and form different embodiments, as would be understood by those in the art. For example, in the following claims, any of the claimed embodiments can be used in any combination.

Specific Details

[0539] In the description provided herein, numerous specific details are set forth. However, it is understood that embodiments of the invention may be practiced without these specific details. In other instances, well-known methods, structures and techniques have not been shown in detail in order not to obscure an understanding of this description.

[0540] It will be appreciated that the computer implemented methods and systems described/illustrated above at least substantially provides a manner in which data generated in an EHR, during an episode of care, may be de-identified (or anonymized) and provided to a user through a secure channel.

[0541] The embodiments described herein, and/or shown in the drawings, are presented by way of example only and are not limiting as to the scope of the invention. Unless otherwise specifically stated, individual aspects and components of the embodiments may be modified, or may have been substituted therefore known equivalents, or as yet unknown substitutes such as may be developed in the future or such as may be found to be acceptable substitutes in

the future. The embodiments may also be modified for a variety of applications while remaining within the scope and spirit of the claimed invention, since the range of potential applications is great, and since it is intended that the present invention be adaptable to many such variations.

Different Instances of Objects

[0542] As used herein, unless otherwise specified the use of the ordinal adjectives "first", "second", "third", etc., to describe a common object, merely indicate that different instances of like objects are being referred to, and are not intended to imply that the objects so described must be in a given sequence, either temporally, spatially, in ranking, or in any other manner.

Comprising and Including

[0543] In the claims which follow and in the preceding description of the invention, except where the context requires otherwise due to express language or necessary implication, the word "comprise" or variations such as "comprises" or "comprising" are used in an inclusive sense, i.e. to specify the presence of the stated features but not to preclude the presence or addition of further features in various embodiments of the invention.

[0544] Any one of the terms: including or which includes or that includes as used herein is also an open term that also means including at least the elements/features that follow the term, but not excluding others. Thus, including is synonymous with and means comprising.

Scope of Invention

[0545] Thus, while there has been described what are believed to be the preferred embodiments of the invention, those skilled in the art will recognize that other and further modifications may be made thereto without departing from the spirit of the invention, and it is intended to claim all such changes and modifications as fall within the scope of the invention. For example, any formulas given above are merely representative of procedures that may be used. Functionality may be added or deleted from the block diagrams and operations may be interchanged among functional blocks. Steps may be added or deleted to methods described within the scope of the present invention.

[0546] Although the invention has been described with reference to specific examples, it will be appreciated by those skilled in the art that the invention may be embodied in many other forms.

Chronological order

[0547] For the purpose of this specification, where method steps are described in sequence, the sequence does not necessarily mean that the steps are to be carried out in chronological order in that sequence, unless there is no other logical manner of interpreting the sequence.

Industrial Applicability

[0548] It is apparent from the above, that the arrangements described are applicable to the industries dealing with banking, brokerages, insurance companies, investment companies and Unit Investment Trusts (UIT) etc.

Claims

1. A computer implemented method for processing a financial transaction, the method comprising the steps of:

transmitting one or more documents pertaining to the financial transaction, from a first intermediary server to a first document store;

generating an enriched data record from the one or more documents, at the first intermediary server, and adding the enriched data record into a blockchain, from the first intermediary sever;

requesting generation of a token corresponding to the financial transaction, to a token server, from the first intermediary server, via a messaging bus;

generating the token at the token server and adding the token into the blockchain from the token server;

transmitting the token to the first intermediary server from the token server, via the messaging bus; and

transmitting the token from the first intermediary server to the first document store.

2. The computer implemented method as claimed in claim 1, further comprising the step of sending a first financial message comprising the token, from the first intermediary server to a second intermediary server, indicative of making a payment to a second user.

3. The computer implemented method as claimed in claim 1, further comprising the steps of:

implementing a smart contract at the token server; and

adding the smart contract into the blockchain, from the token server.

4. The computer implemented method as claimed in claim 1, further comprising the steps of:

transmitting the token from the first intermediary server to a first digital device available with a first user;

providing the token to a second user, by the first user;

providing the token to a second intermediary server, from the second digital device;

transmitting the token to a second document store, from the second intermediary server; and

sending a second financial message comprising the token, from the second intermediary server to the first intermediary server, indicative of making a payment to the first user.

5. The computer implemented method as claimed in claim 1, wherein the step of generating the enriched data record comprises:

extracting a plurality of attributes from the one or more documents, at the first intermediary server; and

combining the plurality of attributes to generate the enriched data record, at the first intermediary server.

6. The computer implemented method as claimed in claim 1, wherein the step of generating the enriched data record comprises:

extracting a plurality of attributes from the one or more documents, at the first intermediary server;

de-identifying the plurality of attributes to obtain a plurality of de-identified attributes, at the first intermediary server; and

combining the plurality of de-identified attributes to generate the enriched data record, at the first intermediary server.

7. The computer implemented method as claimed in claim 1, wherein the step of generating the enriched data record comprises:

extracting a plurality of attributes from the one or more documents, at the first intermediary server;

hashing the plurality of attributes to generate a plurality of respective hashes, at the first intermediary server; and

combining the plurality of hashes to generate the enriched data record, at the first intermediary server.

8. The computer implemented method as claimed in claim 1, further comprising the step of assigning a payment risk rating to the token.

9. The computer implemented method as claimed in claim 1, further comprising the steps of:

transmitting one or more first requests, each comprising the token, from the first intermediary server to the second intermediary server, via the messaging bus;

receiving the one or more first requests at the second intermediary server and transmitting the one or more first requests and the token from the second intermediary server to a second document store;

generating one or more first responses, each comprising the token, corresponding to the respective one or more first requests, at the second intermediary server;

transmitting the one or more first responses from the second intermediary server to the first intermediary server, via the messaging bus;

hashing the one or more first requests and the one or more first responses at the second intermediary server to generate one or more first request hashes and one or more first response hashes, respectively;

adding the one or more first request hashes and the one or more first response hashes to the enriched data record in the blockchain, from the second intermediary server; and

receiving the one or more first responses at the first intermediary server and transmitting the one or more first responses to the first document store.

10. The computer implemented method as claimed in claim 9, further comprising the steps of:

hashing the one or more first responses at the first intermediary server to regenerate the one or more first response hashes; and

verifying the one or more first response hashes with the blockchain from the first intermediary server, using the token.

11. The computer implemented method as claimed in claim 9, wherein each one of the one or more first requests are:

encrypted with a second public key and signed with a first public key at the first intermediary server, before transmission to the second intermediary server; and

decrypted with a second private key at the second intermediary server after reception from the first intermediary server; and

wherein each one of the one or more first responses are:

encrypted with the first public key and signed with the second public key at the second intermediary server, before transmission to the first intermediary server; and

decrypted with a first private key at the first intermediary server after reception from the second intermediary server.

12. The computer implemented method as claimed in claim 9, wherein the one or more first responses comprise one or more second regulatory compliance documents pertaining to a second user.

13. The computer implemented method as claimed in claim 1, further comprising the steps of:

transmitting one or more second requests, each comprising the token, from the second intermediary server to the first intermediary server, via the messaging bus;

receiving the one or more second requests at the first intermediary server and transmitting the one or more second requests from the first intermediary server to the first document store;

generating one or more second responses, each comprising the token, corresponding to the respective one or more second requests, at the first intermediary server;

transmitting the one or more second responses from the first intermediary server to the second intermediary server, via the messaging bus;

hashing the one or more second requests and the one or more second responses at the first intermediary server to generate one or more second request hashes and one or more second response hashes, respectively;

adding the one or more second request hashes and the one or more second response hashes to the enriched data record in the blockchain, from the first intermediary server; and

receiving the one or more second responses at the second intermediary server and transmitting the one or more second responses to the second document store.

14. The computer implemented method as claimed in claim 13, further comprising the steps of:

hashing the one or more second responses at the second intermediary server to regenerate the one or more second response hashes; and

verifying the one or more second response hashes with the blockchain from the second intermediary server, using the token.

15. The computer implemented method as claimed in claim 13, wherein each one of the one or more second requests are:

encrypted with a first public key and signed with a second public key at the second intermediary server, before transmission to the first intermediary server; and

decrypted with a first private key at the first intermediary server after reception from the second intermediary server; and

wherein each one of the one or more second responses are:

encrypted with the second public key and signed with the first public key at the first intermediary server, before transmission to the second intermediary server; and

decrypted with a second private key at the second intermediary server after reception from the first intermediary server.

16. The computer implemented method as claimed in claim 11 or 15, further comprising the steps of adding the first public key from the first intermediary server into the blockchain and adding the second public key from the second intermediary server into the blockchain.

17. The computer implemented method as claimed in claim 13, wherein the one or more second responses comprise one or more first regulatory compliance documents pertaining to a first user.

18. A system for processing a financial transaction, the system comprising:

a first intermediary server operably connected to a network and a first document store;

a token server operably connected to the network;

a messaging bus operably connected to the network; and

a blockchain operably connected to the network;

wherein the first intermediary server is configured to:

transmit one or more documents pertaining to the financial transaction, to the first document store;

generate an enriched data record from the one or more documents and add the enriched data record into the blockchain;

request generation of a token corresponding to the financial transaction, to the token server, via the messaging bus; and

transmit the token to the first document store;

wherein the token server is configured to:

generate the token and add the token into the blockchain; and

transmit the token to the first intermediary server, via the messaging bus.

19. The system as claimed in claim 18, further comprising a second intermediary server operably connected to the network and a second document store;

wherein the first intermediary server is further configured to send a first financial message comprising the token, to the second intermediary server, indicative of making a payment to a second user.

20. The system as claimed in claim 18, wherein the token server is further configured to:

implement a smart contract; and

add the smart contract into the blockchain.

21. The system as claimed in claim 18, further comprising:

a first digital device operably connected to the network;

a second digital device operably connected to the network;

a second intermediary server operably connected to the network and a second document store;

wherein the first intermediary server is further configured to:

transmit the token to the first digital device;

wherein the first digital device comprises a first memory and a first processor operably connected to the first memory, the first memory comprising a first computer program code, the first computer program code when executed by the first processor, instructs the first processor to:

receive the token from the first intermediary server;

provide the token to the second digital device;

wherein the second digital device comprises a second memory and a second processor operably connected to the second memory, the second memory comprising a second computer program code, the second computer program code when executed by the second processor, instructs the second processor to:

receive the token from the first digital device; and

provide the token to the second intermediary server; and

wherein the second intermediary server is configured to:

receive the token from the second digital device;

transmit the token to the second document store; and

send a second financial message comprising the token, to the first intermediary server, indicative of making a payment to a first user.

22. The system as claimed in claim 18, wherein for generation of the enriched data record, the first intermediary server is configured to:

extract a plurality of attributes from the one or more documents; and

combine the plurality of attributes to generate the enriched data record.

23. The system as claimed in claim 18, wherein for generation of the enriched data record, the first intermediary server is configured to:

extract a plurality of attributes from the one or more documents;

de-identify the plurality of attributes to obtain a plurality of de-identified attributes; and

combine the plurality of de-identified attributes to generate the enriched data record.

24. The system as claimed in claim 18, wherein for generation of the enriched data record, the first intermediary server is configured to:

extract a plurality of attributes from the one or more documents;

hash the plurality of attributes to generate a plurality of respective hashes; and

combine the plurality of hashes to generate the enriched data record.

25. The system as claimed in claim 18, wherein the first intermediary server is further configured to assign a payment risk rating to the token.

26. The system as claimed in claim 18, further comprising:

a second intermediary server operably connected to the network and a second document store;

wherein the first intermediary server is configured to:

transmit one or more first requests, each comprising the token, to the second intermediary server, via the messaging bus; and

receive one or more first responses and transmit the one or more first responses to the first document store;

wherein the second intermediary server is configured to:

receive the one or more first requests from the first intermediary server and transmit the one or more first requests and the token to the second document store;

generate the one or more first responses, each comprising the token, corresponding to the respective one or more first requests;

transmit the one or more first responses to the first intermediary server, via the messaging bus;

hash the one or more first requests and the one or more first responses to generate one or more first request hashes and one or more first response hashes, respectively; and

add the one or more first request hashes and the one or more first response hashes to the enriched data record in the blockchain.

27. The system as claimed in claim 26, wherein the first intermediary server is further configured to:

hash the one or more first responses to regenerate the one or more first response hashes; and

verify the one or more first response hashes with the blockchain, using the token.

28. The system as claimed in claim 26, wherein the first intermediary server is further configured to:

encrypt each one of the one or more first requests with a second public key and sign each one of the one or more first requests with a first public key, before transmission to the second intermediary server; and

decrypt each one of the one or more first responses with a first private key after reception from the second intermediary server;

wherein the second intermediary server is further configured to:

encrypt the each one of the one or more first responses with the first public key and sign the each one of the one or more first responses with the second public key, before transmission to the first intermediary server; and

decrypt the each one of the one or more first requests with a second private key after reception from the first intermediary server.

29. The system as claimed in claim 26, wherein the one or more first responses comprise one or more second regulatory compliance documents pertaining to a second user.

30. The system as claimed in claim 18, further comprising:

a second intermediary server connected to the network and a second document store;

wherein the second intermediary server is configured to:

transmit one or more second requests, each comprising the token, to the first intermediary server, via the messaging bus;

receive one or more second responses and transmit the one or more second responses to the second document store;

wherein the first intermediary server is further configured to:

receive the one or more second requests and transmit the one or more second requests to the first document store;

generate the one or more second responses, each comprising the token, corresponding to the respective one or more second requests;

transmit the one or more second responses to the second intermediary server, via the messaging bus;

hash the one or more second requests and the one or more second responses to generate one or more second request hashes and one or more second response hashes, respectively; and

add the one or more second request hashes and the one or more second response hashes to the enriched data record in the blockchain.

31. The system as claimed in claim 30, wherein the second intermediary server is further configured to:

hash the one or more second responses to regenerate the one or more second response hashes; and

verify the one or more second response hashes with the blockchain, using the token.

32. The system as claimed in claim 30, wherein the second intermediary server is further configured to:

encrypt each one of the one or more second requests with a first public key and sign each one of the one or more second requests with a second public key, before transmission to the first intermediary server; and

decrypt each one of the one or more second responses with a second private key after reception from the first intermediary server;

wherein the first intermediary server is further configured to:

encrypt the each one of the one or more second responses with the second public key and sign the each one of the one or more second responses with the first public key, before transmission to the second intermediary server; and

decrypt the each one of the one or more second requests with a first private key after reception from the second intermediary server.

33. The system as claimed in claim 28 or 32, wherein the first intermediary server is further configured to add the first public key into the blockchain and the second intermediary server is further configured to add the second public key into the blockchain.

34. The system as claimed in claim 30, wherein the one or more second responses comprise one or more first regulatory compliance documents pertaining to a first user.

35. A token server for facilitating processing of a financial transaction, operably connected to a network and configured to generate a token, add the token into a blockchain and transmit the token to a first intermediary server, via a messaging bus.

36. The token server as claimed in claim 35, further configured to:

implement a smart contract; and

add the smart contract into the blockchain

37. A first intermediary server for facilitating processing of a financial transaction, operably connected to a network and a first document store, and configured to:

transmit one or more documents pertaining to the financial transaction, to the first document store;

generate an enriched data record from the one or more documents and add the enriched data record into a blockchain;

request generation of a token corresponding to the financial transaction, to a token server, via a messaging bus; and

transmit the token to the first document store.

38. The first intermediary server as claimed in claim 37, further configured to send a first financial message comprising the token, to a second intermediary server, indicative of making a payment to a second user.

39. The first intermediary server as claimed in claim 37, further configured to transmit the token to a first digital device.

40. The first intermediary server as claimed in claim 37, wherein for generation of the enriched data record, the first intermediary server is configured to:

extract a plurality of attributes from the one or more documents; and

combine the plurality of attributes to generate the enriched data record.

41. The first intermediary server as claimed in claim 37, wherein for generation of the enriched data record, the first intermediary server is configured:

extract a plurality of attributes from the one or more documents;

de-identify the plurality of attributes to obtain a plurality of de-identified attributes; and

combine the plurality of de-identified attributes to generate the enriched data record.

42. The first intermediary server as claimed in claim 37, wherein for generation of the enriched data record, the first intermediary server is configured to:

extract a plurality of attributes from the one or more documents;

hash the plurality of attributes to generate a plurality of respective hashes; and

combine the plurality of hashes to generate the enriched data record.

43. The first intermediary server as claimed in claim 37, further configured to assign a payment risk rating to the token.

44. The first intermediary server as claimed in claim 37, further configured to:

transmit one or more first requests, each comprising the token, to a second intermediary server, via the messaging bus; and

receive one or more first responses from the second intermediary server and transmit the one or more first responses to the first document store.

45. The first intermediary server as claimed in claim 44, wherein the one or more first responses comprise one or more second regulatory compliance documents pertaining to a second user.

46. The first intermediary server as claimed in claim 44, further configured to:

hash the one or more first responses to regenerate one or more first response hashes; and

verify the one or more first response hashes with the blockchain, using the token.

47. The first intermediary server as claimed in claim 44, further configured to:

encrypt each one of the one or more first requests with a second public key and sign each one of the one or more first requests with a first public key, before transmission to the second intermediary server; and

decrypt each one of the one or more first responses with a first private key after reception from the second intermediary server.

48. The first intermediary server as claimed in claim 37, further configured to:

receive the one or more second requests from a second intermediary server and transmit the one or more second requests to the first document store;

generate one or more second responses, each comprising the token, corresponding to the respective one or more second requests;

transmit the one or more second responses to the second intermediary server, via the messaging bus;

hash the one or more second requests and the one or more second responses to generate one or more second request hashes and one or more second response hashes, respectively; and

add the one or more second request hashes and the one or more second response hashes to the enriched data record in the blockchain.

49. The first intermediary server as claimed in claim 48, wherein the first intermediary server is further configured to:

encrypt each one of the one or more second responses with a second public key and sign the each one of the one or more second responses with a first public key, before transmission to the second intermediary server; and

decrypt each one of the one or more second requests with a first private key after reception from the second intermediary server.

50. The first intermediary server as claimed in claims 47 or 49, further configured to add the first public key into the blockchain.

51. A second intermediary server for facilitating processing of a financial transaction, operably connected to a network and a second document store, and configured to:

receive the token from the second digital device;

transmit the token to the second document store; and

send a second financial message comprising the token to a first intermediary server, indicative of making a payment to a first user.

52. A second intermediary server for facilitating processing of a financial transaction, operably connected to a network and a second document store, and configured to:

receive one or more first requests, each comprising a token, from a first intermediary server and transmit the one or more first requests and the token to the second document store;

generate the one or more first responses, each comprising the token, corresponding to the respective one or more first requests;

transmit the one or more first responses to the first intermediary server, via a messaging bus;

hash the one or more first requests and the one or more first responses to generate one or more first request hashes and one or more first response hashes, respectively; and

add the one or more first request hashes and the one or more first response hashes to the enriched data record in the blockchain.

53. The second intermediary server as claimed in claim 52, further configured to:

encrypt each one of the one or more first responses with a first public key and sign the each one of the one or more first responses with a second public key, before transmission to the first intermediary server; and

decrypt each one of the one or more first requests with a second private key after reception from the first intermediary server.

54. A second intermediary server for facilitating processing of a financial transaction, operably connected to a network and a second document store, and configured to:

transmit one or more second requests, each comprising a token, to a first intermediary server, via a messaging bus; and

receive one or more second responses from the first intermediary server and transmit the one or more second responses to the second document store.

55. The second intermediary server as claimed in claim 54, further configured to:

hash the one or more second responses to regenerate one or more second response hashes; and

verify the one or more second response hashes with the blockchain, using the token.

56. The second intermediary server as claimed in claim 54, further configured to:

encrypt each one of the one or more second requests with a first public key and sign each one of the one or more second requests with a second public key, before transmission to the first intermediary server; and

decrypt each one of the one or more second responses with a second private key after reception from the first intermediary server.

57. The second intermediary server as claimed in claims 53 or 56, further configured to add the second public key into the blockchain.

58. The second intermediary server as claimed in claim 54, wherein the one or more second responses comprise one or more first regulatory compliance documents pertaining to a first user.

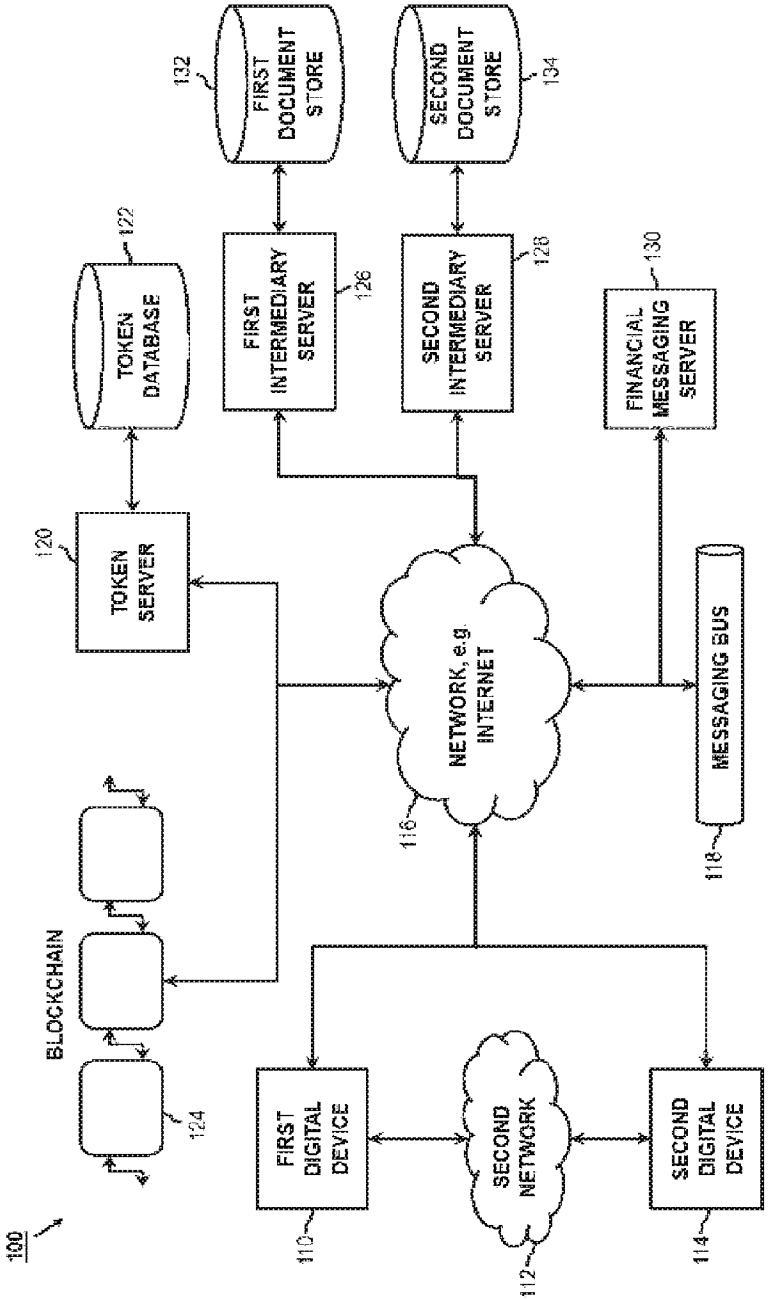

100
FIRST DIGITAL DEVICE
110
SECOND NETWORK
112
SECOND DIGITAL DEVICE
114
BLOCKCHAIN
124
NETWORK, e.g. INTERNET
116
MESSAGING BUS
118
TOKEN SERVER
120
TOKEN DATABASE
122
FIRST INTERMEDIARY SERVER
126
SECOND INTERMEDIARY SERVER
128
FINANCIAL MESSAGING SERVER
130
FIRST DOCUMENT STORE
132
SECOND DOCUMENT STORE
134

FIG. 1

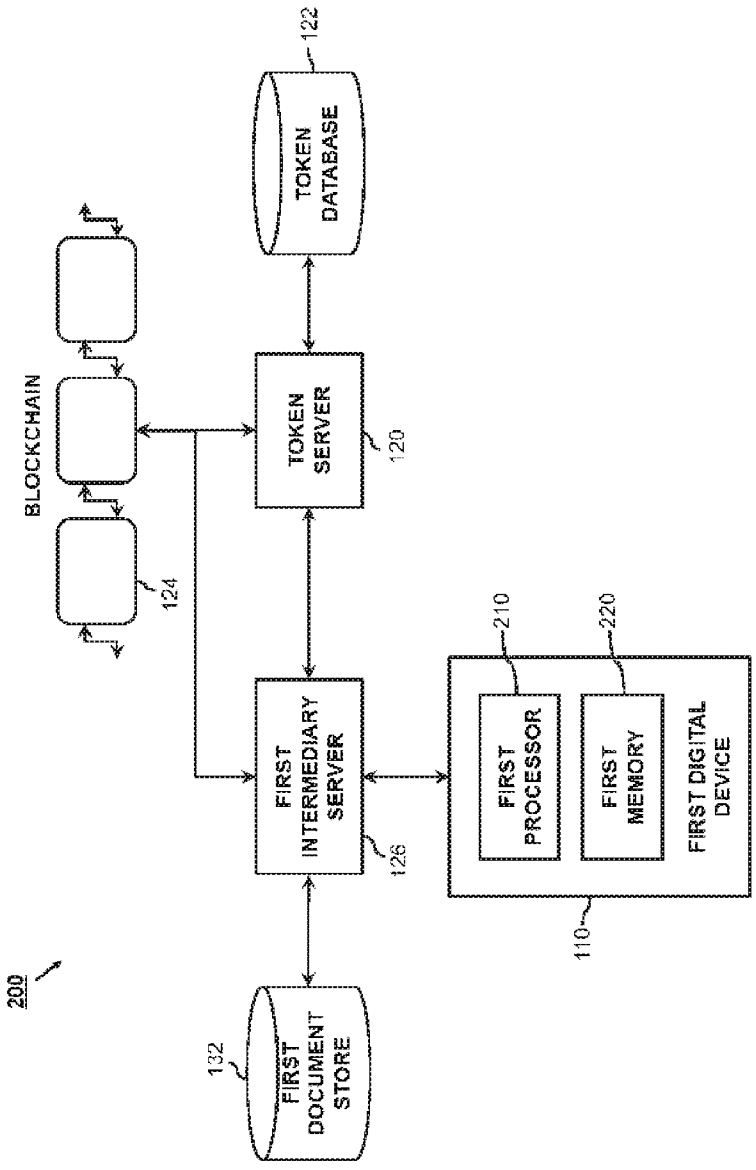

200
BLOCKCHAIN
124
TOKEN DATABASE
122
TOKEN SERVER
120
FIRST INTERMEDIARY SERVER
126
FIRST DOCUMENT STORE
132
FIRST PROCESSOR
210
FIRST MEMORY
220
FIRST DIGITAL DEVICE
110

FIG. 2

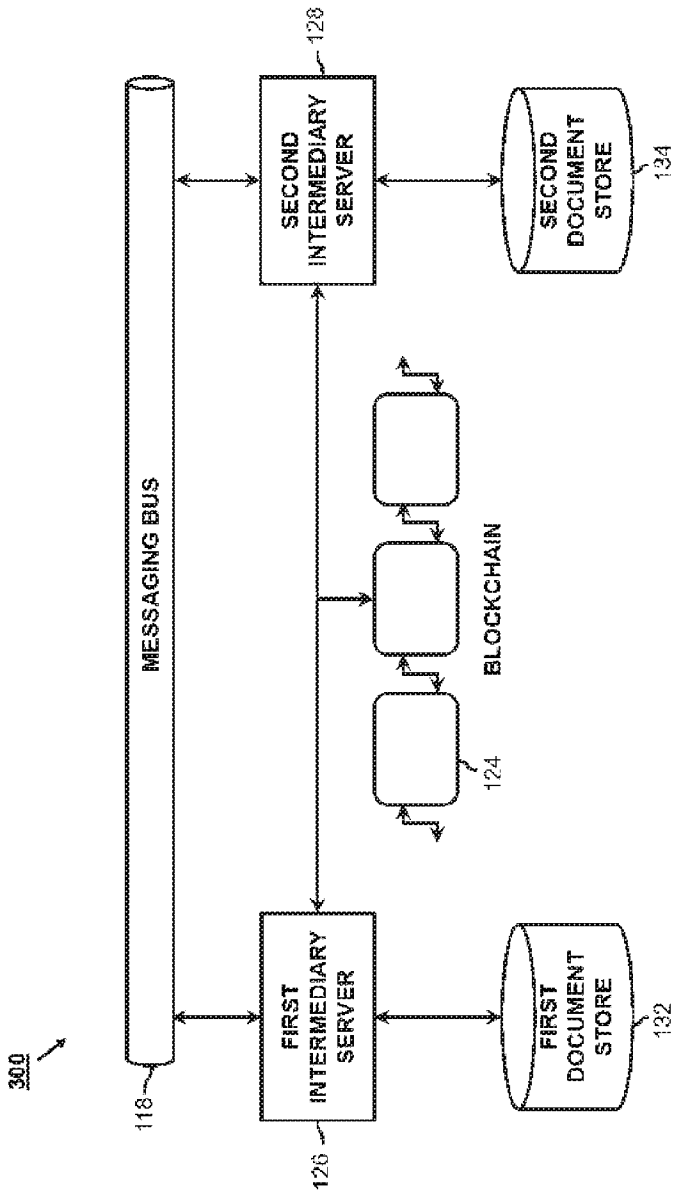

300
MESSAGING BUS
118
SECOND INTERMEDIARY SERVER
128
SECOND DOCUMENT STORE
134
BLOCKCHAIN
124
FIRST INTERMEDIARY SERVER
126
FIRST DOCUMENT STORE
132

FIG. 3

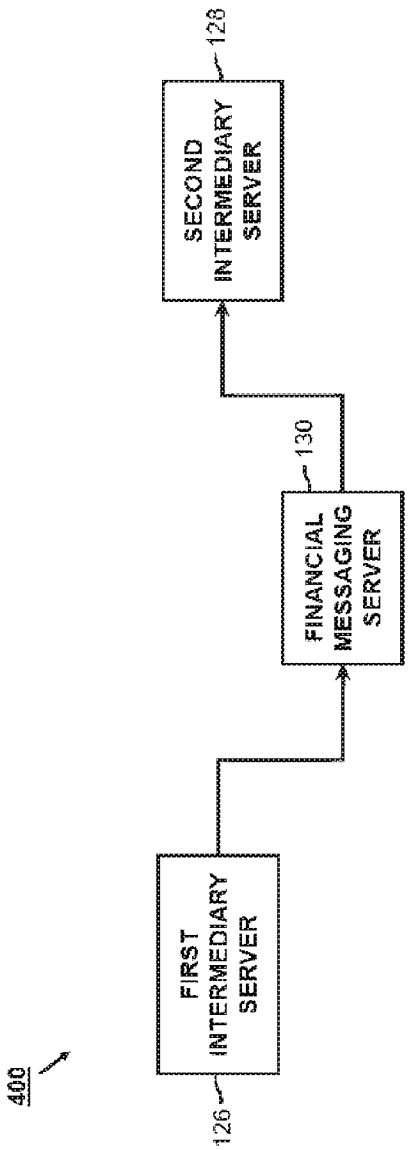

400
FIRST INTERMEDIARY SERVER
126
FINANCIAL MESSAGING SERVER
130
SECOND INTERMEDIARY SERVER
128

FIG. 4

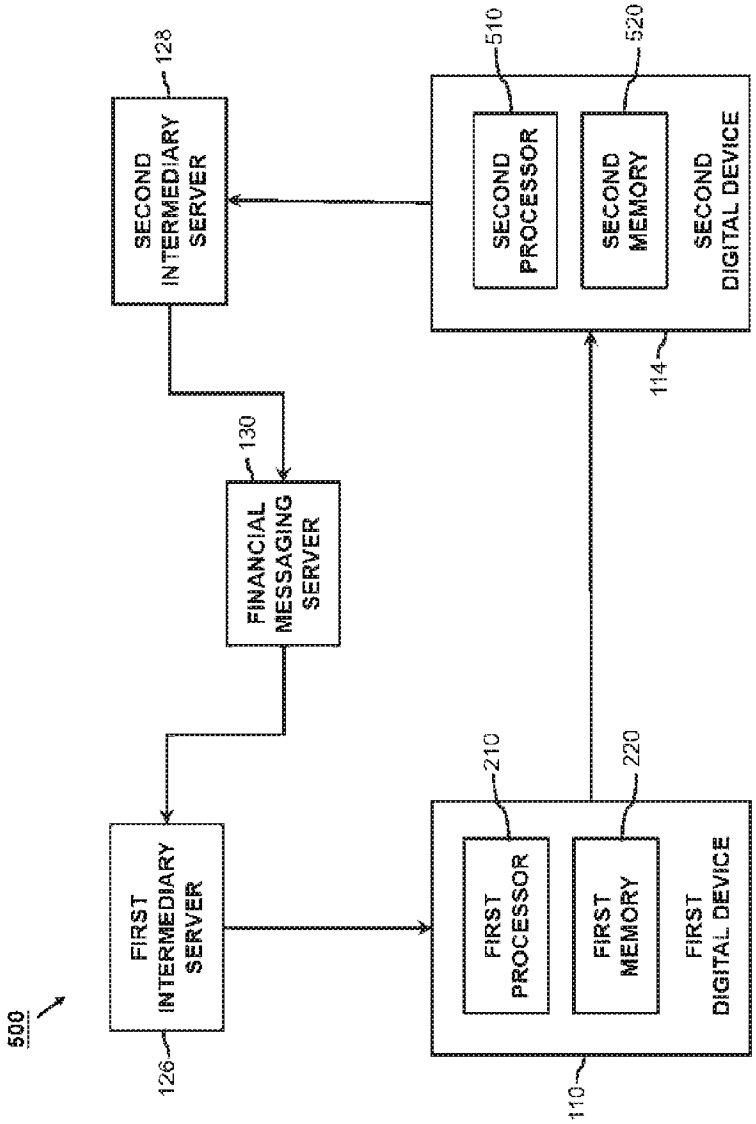

500
FIRST INTERMEDIARY SERVER
126
FINANCIAL MESSAGING SERVER
130
SECOND INTERMEDIARY SERVER
128
FIRST PROCESSOR
210
FIRST MEMORY
220
FIRST DIGITAL DEVICE
110
SECOND PROCESSOR
510
SECOND MEMORY
520
SECOND DIGITAL DEVICE
114

FIG. 5

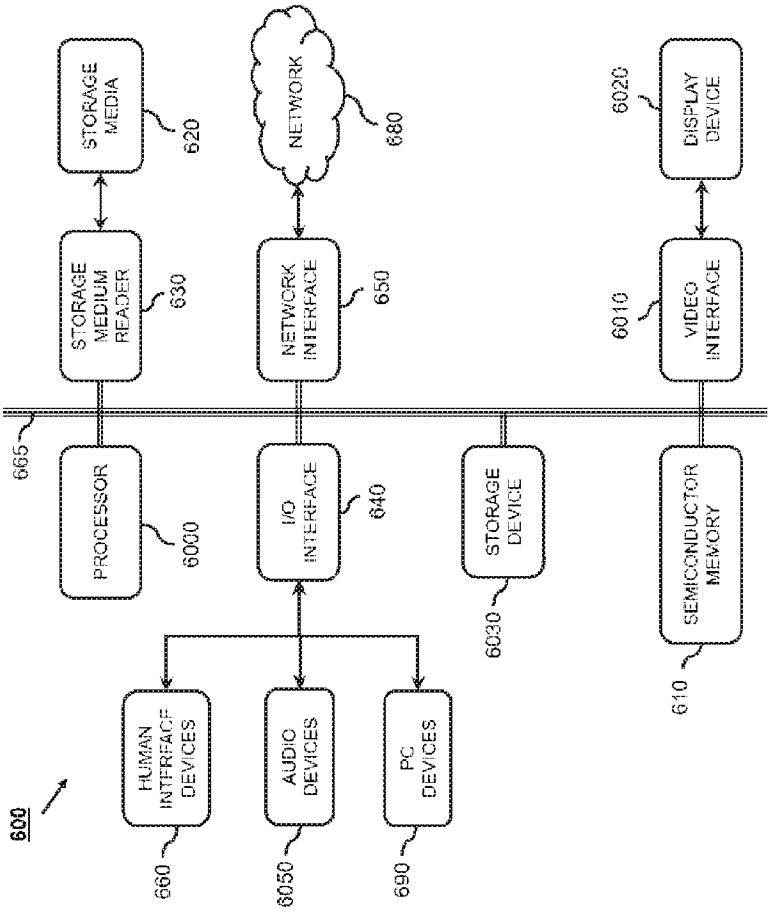

600
665
PROCESSOR
6000
STORAGE MEDIUM READER
630
STORAGE MEDIA
620
I/O INTERFACE
640
NETWORK INTERFACE
650
NETWORK
680
STORAGE DEVICE
6030
VIDEO INTERFACE
6010
DISPLAY DEVICE
6020
SEMICONDUCTOR MEMORY
610
HUMAN INTERFACE DEVICES
660
AUDIO DEVICES
6050
PC DEVICES
690

FIG. 6

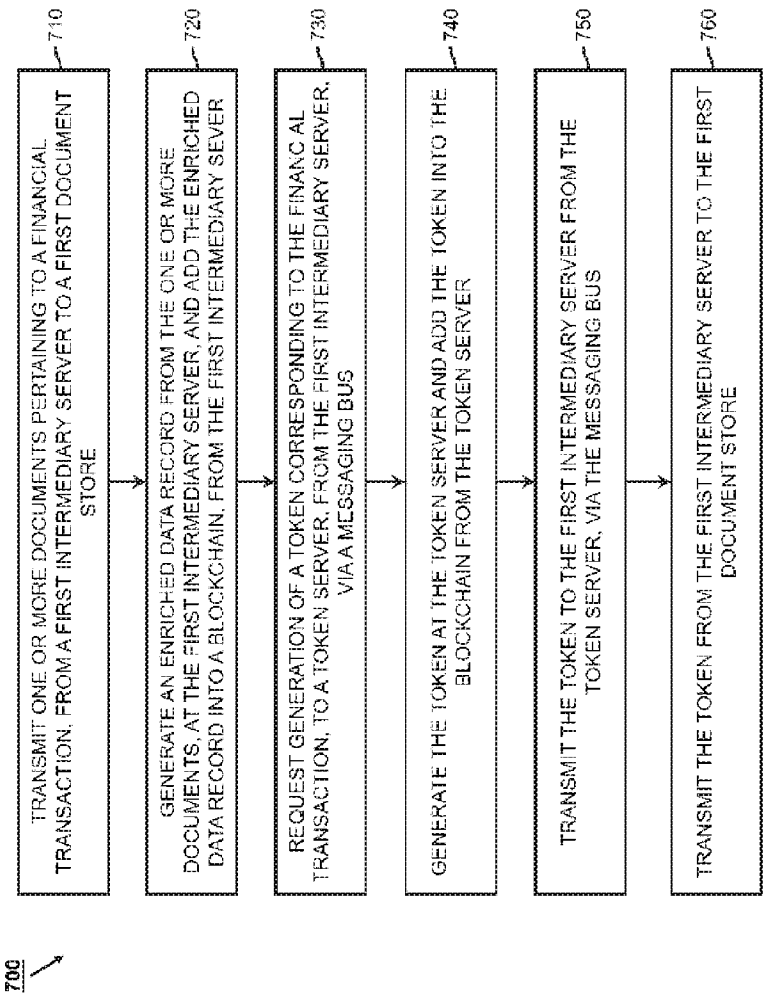

700
710
TRANSMIT ONE OR MORE DOCUMENTS PERTAINING TO A FINANCIAL TRANSACTION, FROM A FIRST INTERMEDIARY SERVER TO A FIRST DOCUMENT STORE
720
GENERATE AN ENRICHED DATA RECORD FROM THE ONE OR MORE DOCUMENTS, AT THE FIRST INTERMEDIARY SERVER, AND ADD THE ENRICHED DATA RECORD INTO A BLOCKCHAIN, FROM THE FIRST INTERMEDIARY SEVER
730
REQUEST GENERATION OF A TOKEN CORRESPONDING TO THE FINANC AL TRANSACTION, TO A TOKEN SERVER, FROM THE FIRST INTERMEDIARY SERVER, VIA A MESSAGING BUS
740
GENERATE THE TOKEN AT THE TOKEN SERVER AND ADD THE TOKEN INTO THE BLOCKCHAIN FROM THE TOKEN SERVER
750
TRANSMIT THE TOKEN TO THE FIRST INTERMEDIARY SERVER FROM THE TOKEN SERVER, VIA THE MESSAGING BUS
760
TRANSMIT THE TOKEN FROM THE FIRST INTERMEDIARY SERVER TO THE FIRST DOCUMENT STORE

FIG. 7

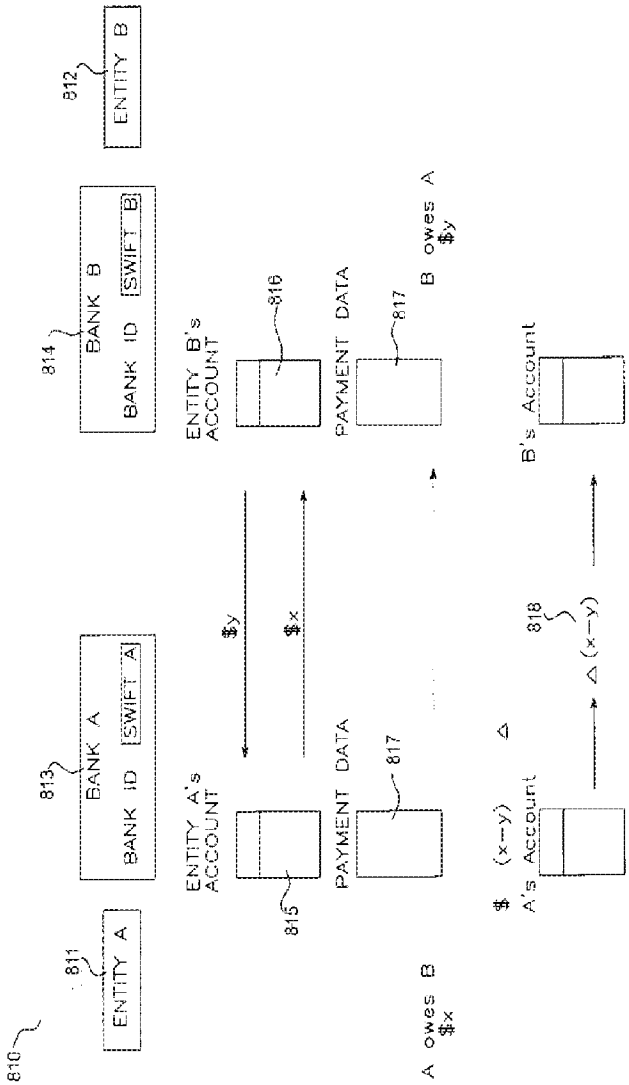


FIG. 8A
[PRIOR ART]

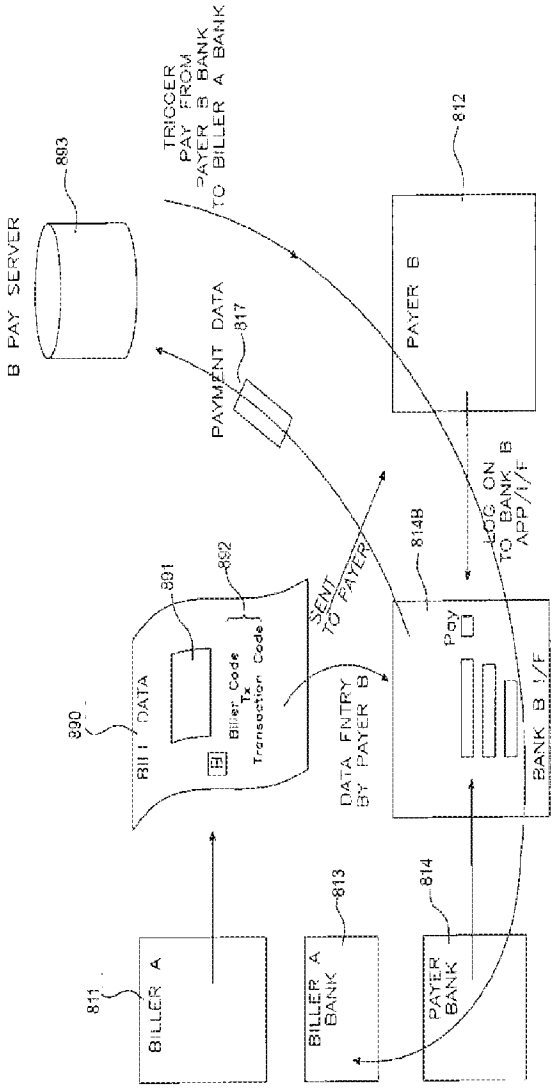


FIG. 8B
[PRIOR ART]

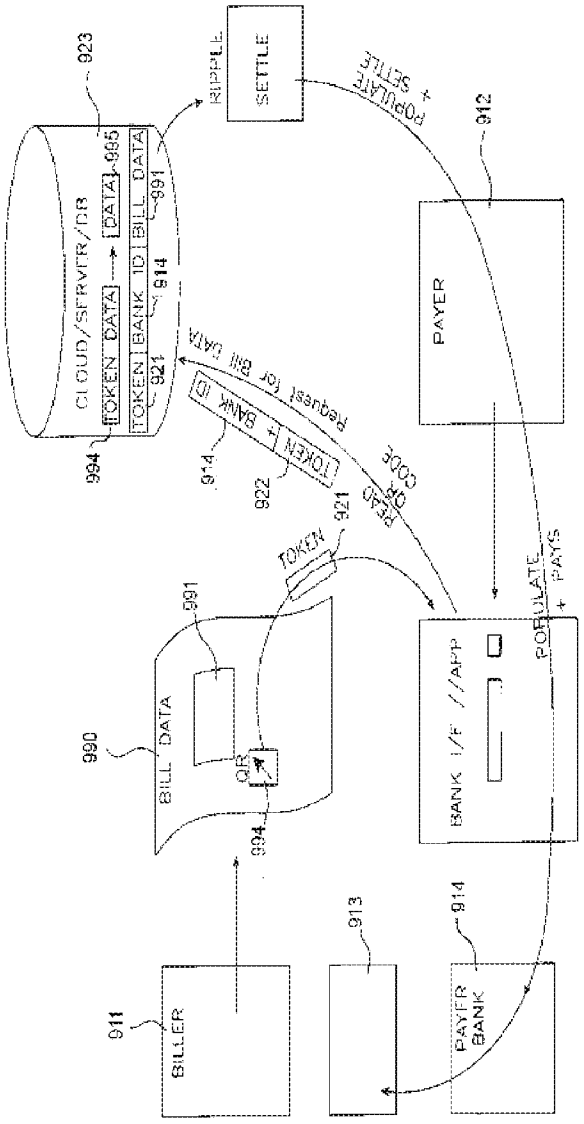

923
CLOUD/SERVER/DB
TOKEN
DATA
BANK ID
DATA
BILL DATA
991
914
921
994
RIPPLE
SETTLE
POPULATE
+ SETTLE
912
PAYER
Request for Bill DATA
TOKEN + BANK ID
914
922
921
QR CODE
TOKEN
991
990
BILL DATA
QR
994
POPULATE
+ PAYS
BANK I/F //APP
913
914
911
BILLER
PAYER BANK

FIG. 9A

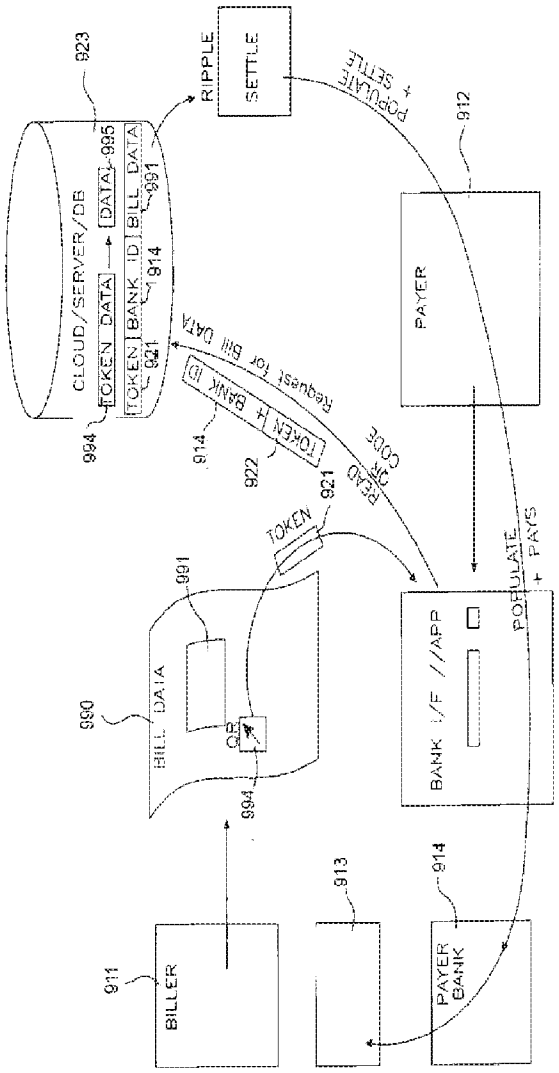

923
RIPPLE
SETTLE
POPULATE + SETTLE
912
CLOUD/SERVER/DB
DATA 995
TOKEN DATA
BANK ID BILL DATA
991
914
921
994
PAYER
Request for Bill DATA
TOKEN + BANK ID
914
922
READ QR CODE
921
TOKEN
991
990
BILL DATA
QR
994
BANK I/F //APP
POPULATE + PAYS
913
914
911
BILLER
PAYER BANK

FIG. 9B

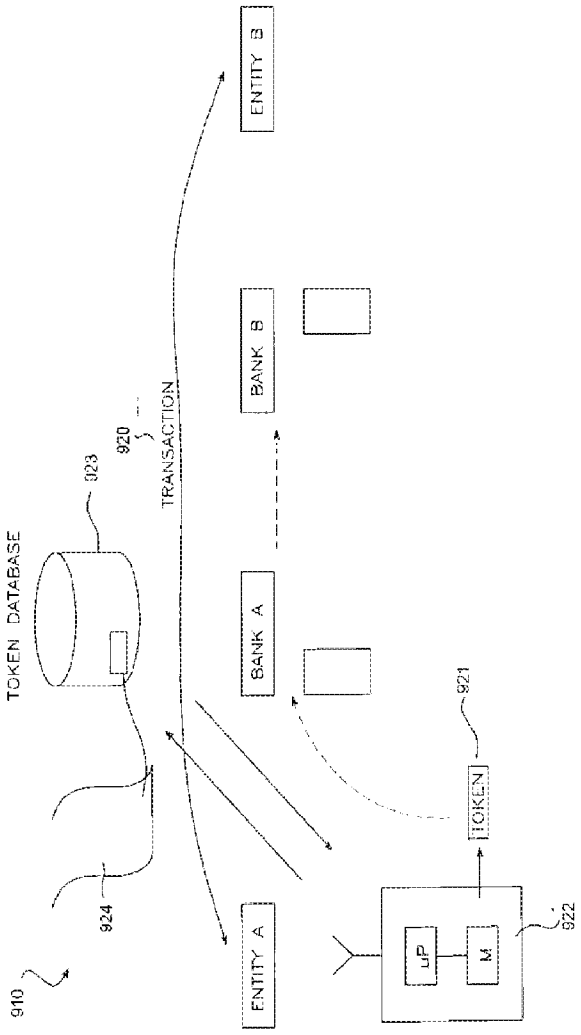

ENTITY B
BANK B
BANK A
TRANSACTION
920
923
TOKEN DATABASE
924
910
ENTITY A
921
TOKEN
922
uP
M

FIG. 9C

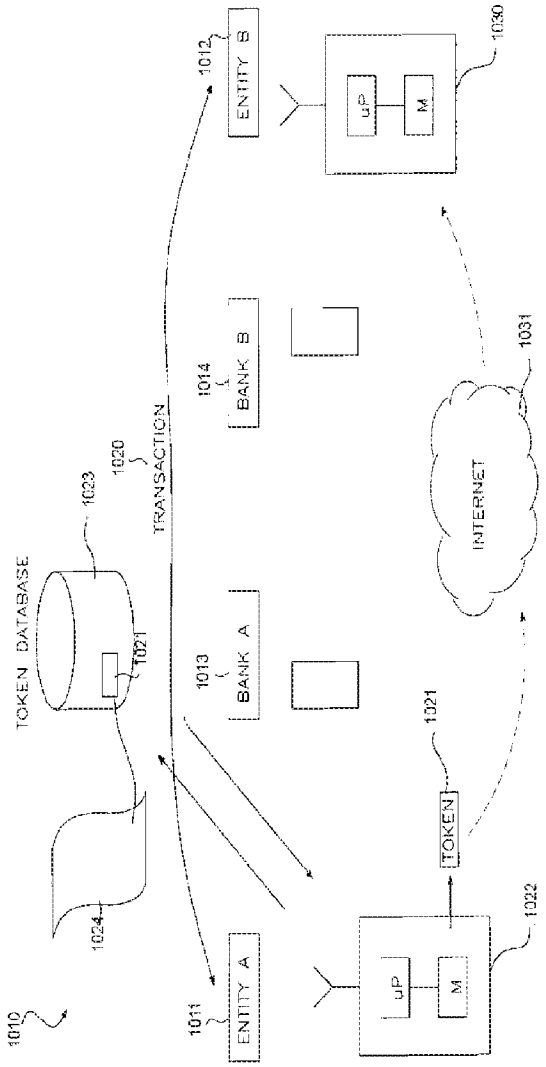

1010
1011
ENTITY A
1012
ENTITY B
1013
BANK A
1014
BANK B
1020
TRANSACTION
1021
TOKEN
1022
uP
M
1023
TOKEN DATABASE
1024
1030
1031
INTERNET

FIG. 10A

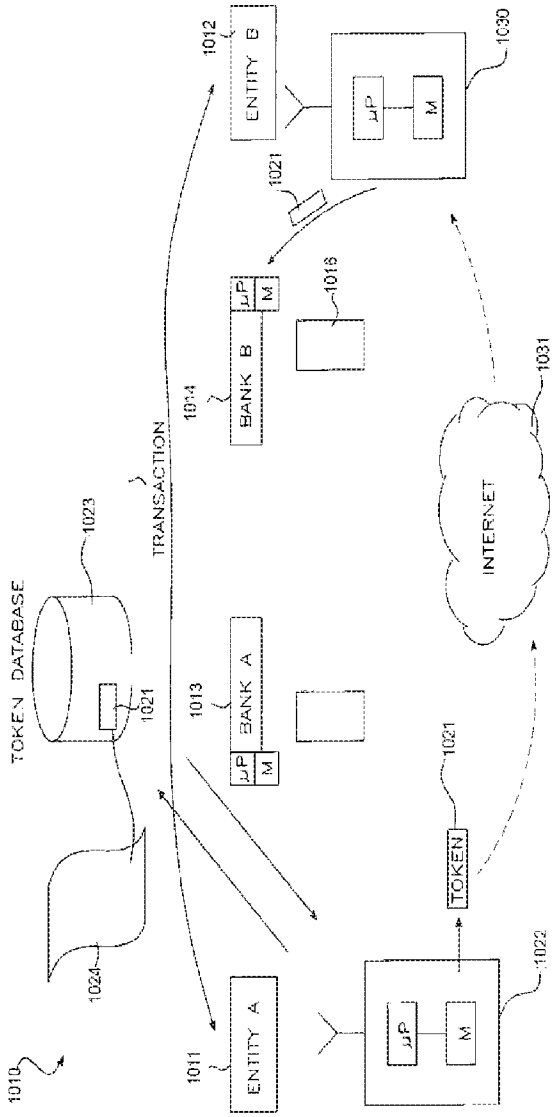

1012
ENTITY B
μP
M
1030
1021
1016
BANK B
1014
TRANSACTION
1031
INTERNET
1023
TOKEN DATABASE
1021
1013
BANK A
1021
TOKEN
1024
1022
1010
1011
ENTITY A

FIG. 10B

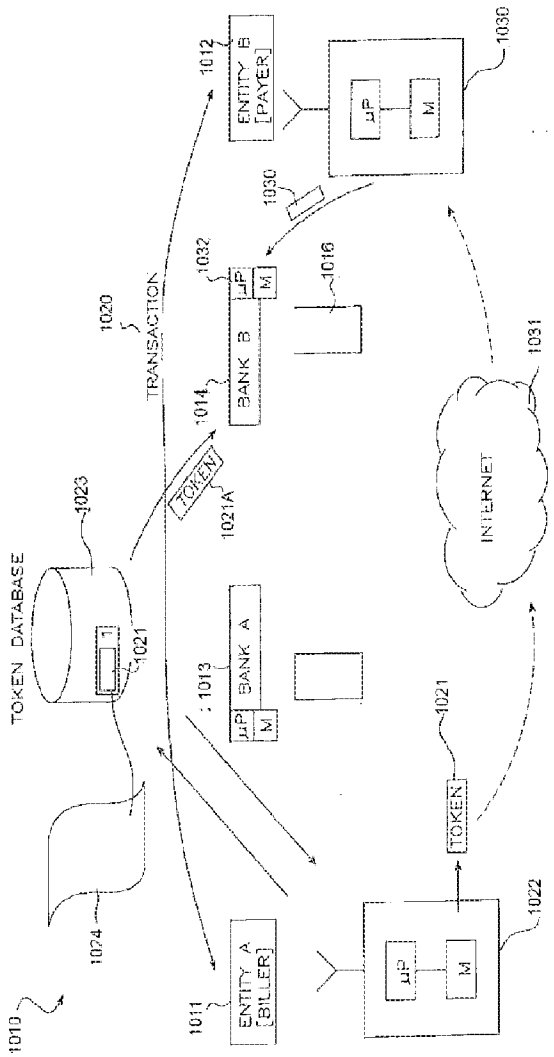

1010
1011
ENTITY A [BILLER]
1012
ENTITY B [PAYER]
1013
BANK A
1014
BANK B
1016
1020
TRANSACTION
1021
1021A
TOKEN
1022
1023
TOKEN DATABASE
1024
1030
1031
INTERNET
1032
µP
M

FIG. 10C

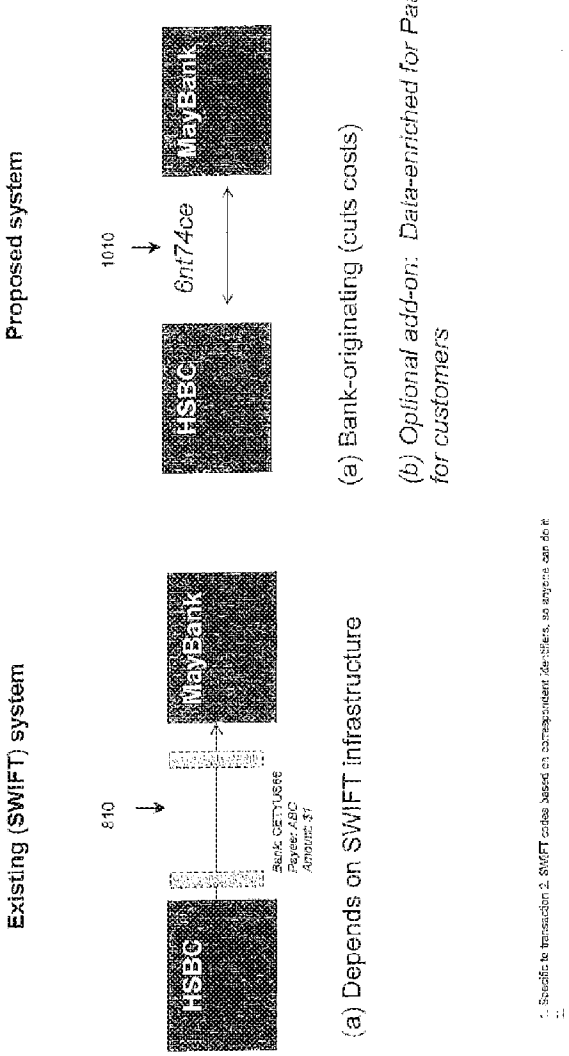

Existing (SWIFT) system
Proposed system
HSBC
810
MayBank
Bank: CBTYUS66
Payee: ABC
Amount: $Y
HSBC
1010
6nf74ce
MayBank
(a) Depends on SWIFT infrastructure
(a) Bank-originating (cuts costs)
(b) Optional add-on: Data-enriched for PaaS for customers

FIG. 11

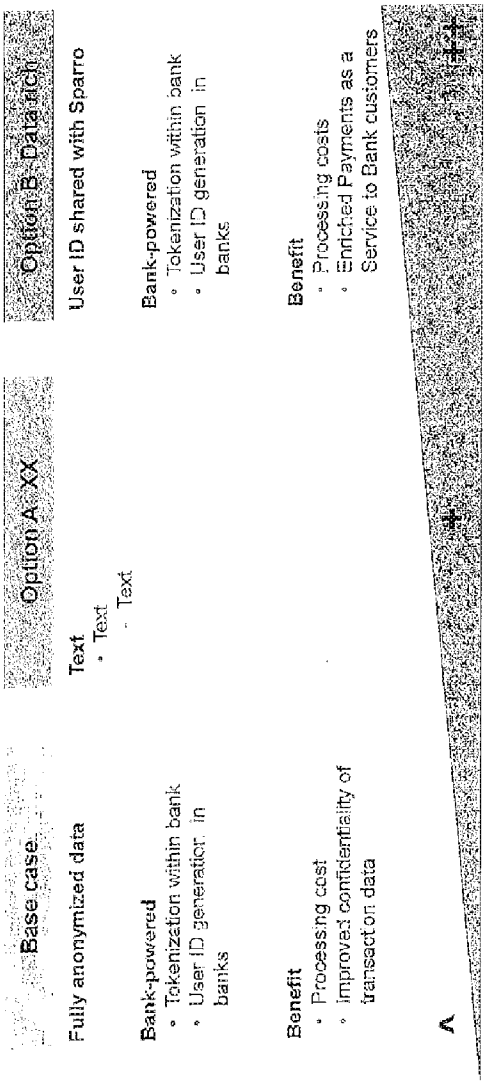

Base case
Fully anonymized data
Bank-powered
Tokenization within bank
User ID generation in banks
Benefit
Processing cost
Improved confidentiality of transaction data
Option A: XX
Text
Text
Text
Bank-powered
Tokenization within bank
User ID generation in banks
Benefit
Processing costs
Enriched Payments as a Service to Bank customers
Option B: Data rich
User ID shared with Sparro

FIG. 12

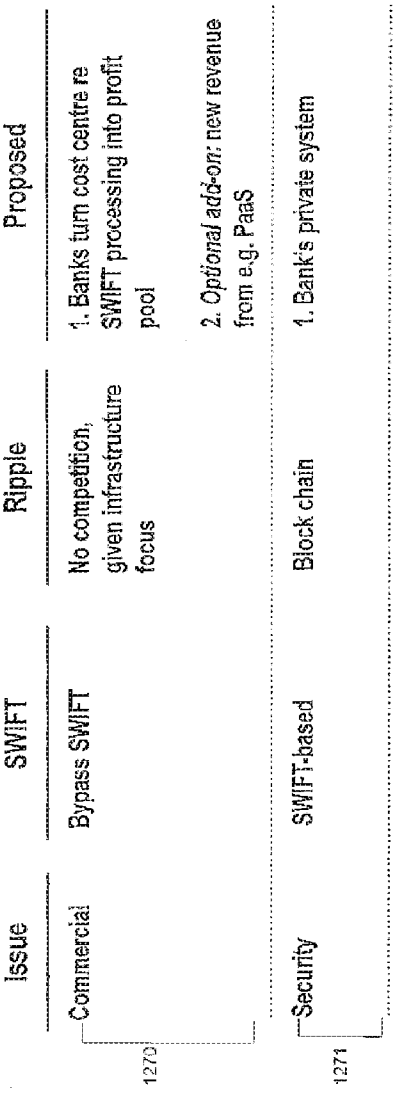

Issue
SWIFT
Ripple
Proposed
Commercial
Bypass SWIFT
No competition, given infrastructure focus
1. Banks turn cost centre re SWIFT processing into profit pool
2. Optional add-on: new revenue from e.g. PaaS
1270
Security
SWIFT-based
Block chain
1. Bank's private system
1271
Technical
Committed infrastructure spend is slow & expensive
Private gateway establishment
Sparro (anonymized) messaging
1272

FIG. 13

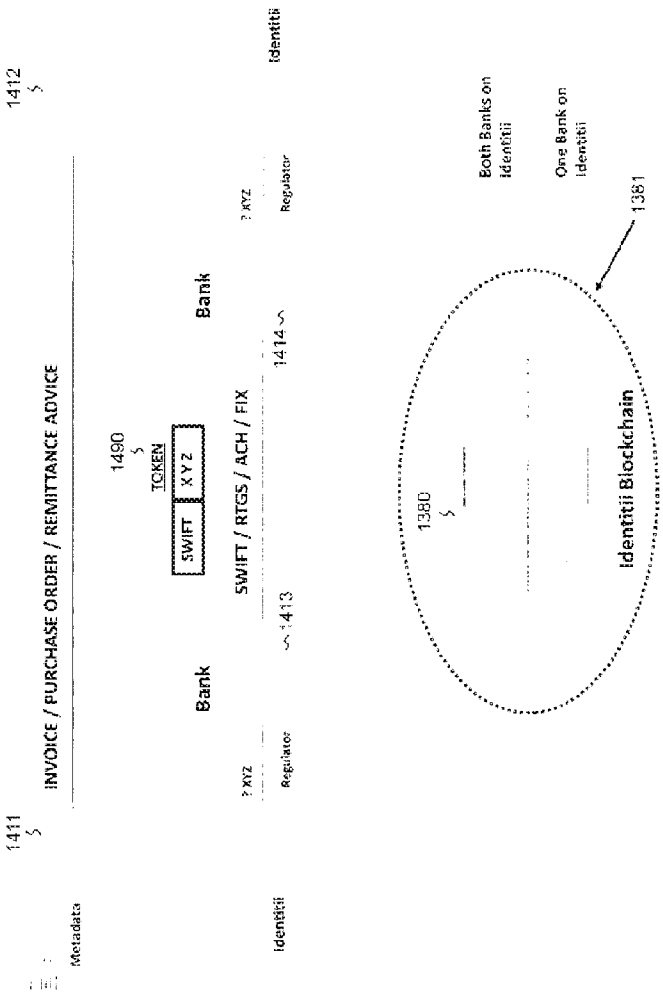

1412
INVOICE / PURCHASE ORDER / REMITTANCE ADVICE
1411
Metadata
1490
TOKEN
SWIFT
XYZ
Bank
Bank
SWIFT / RTGS / ACH / FIX
1414
1413
Identitii
Regulator
? XYZ
Identitii
Regulator
? XYZ
Both Banks on Identitii
One Bank on Identitii
1381
1380
Identitii Blockchain

FIG. 14

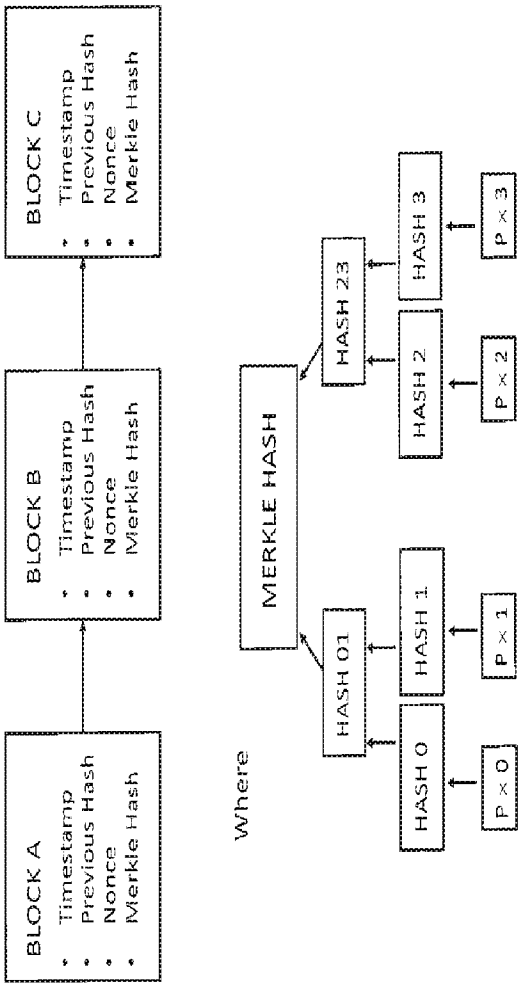

BLOCK A
Timestamp
Previous Hash
Nonce
Merkle Hash
BLOCK B
Timestamp
Previous Hash
Nonce
Merkle Hash
BLOCK C
Timestamp
Previous Hash
Nonce
Merkle Hash
Where
MERKLE HASH
HASH 01
HASH 23
HASH 0
HASH 1
HASH 2
HASH 3
P × 0
P × 1
P × 2
P × 3

FIG. 15A

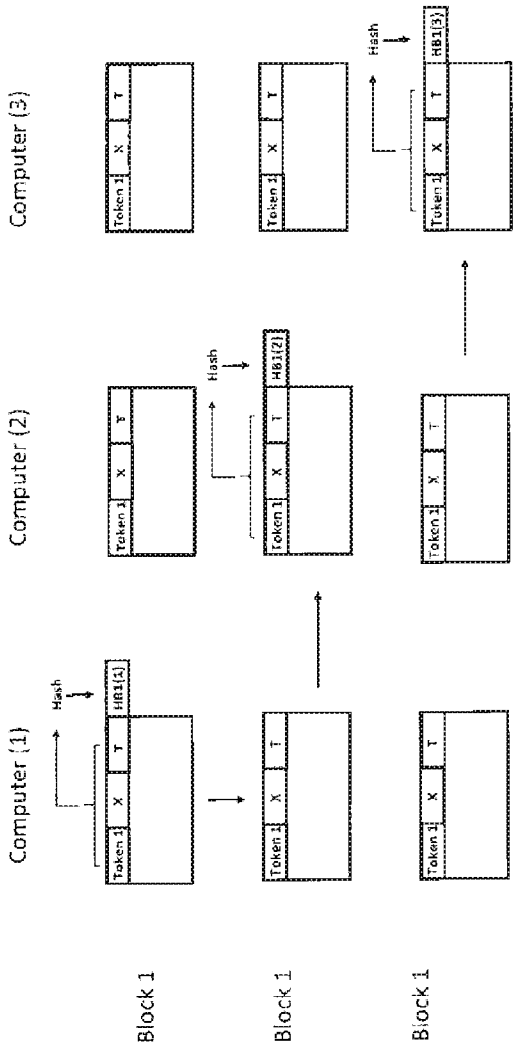

Computer (1)
Computer (2)
Computer (3)
Hash
HB1(1)
HB1(2)
HB1(3)
Token 1
X
T
Block 1
Block 1
Block 1

FIG. 15B

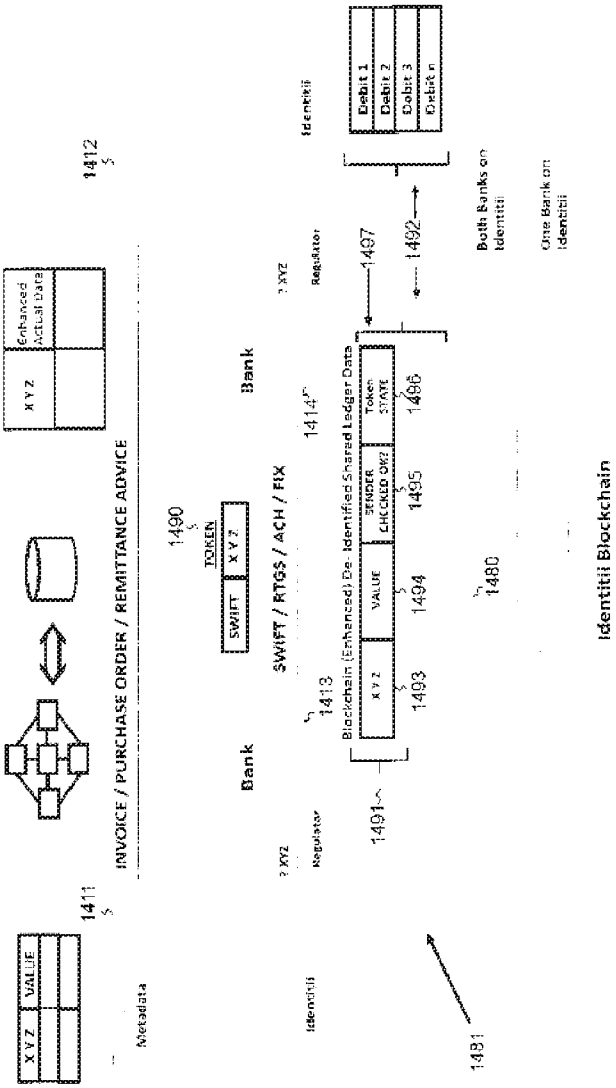

1412
Enhanced Actual Data
XYZ
INVOICE / PURCHASE ORDER / REMITTANCE ADVICE
1411
XYZ
VALUE
Metadata
1490
TOKEN
SWIFT
XYZ
SWIFT / RTGS / ACH / FIX
Bank
Bank
1414
1413
Identitii
Regulator
XYZ
Identitii
Regulator
XYZ
Blockchain (Enhanced) De- Identified Shared Ledger Data
XYZ
VALUE
SENDER CHECKED OK?
Token STATE
1493
1494
1495
1496
1497
1492
Debit 1
Debit 2
Debit 3
Debit n
Both Banks on Identitii
One Bank on Identitii
1491
1480
1481
Identitii Blockchain

FIG. 16

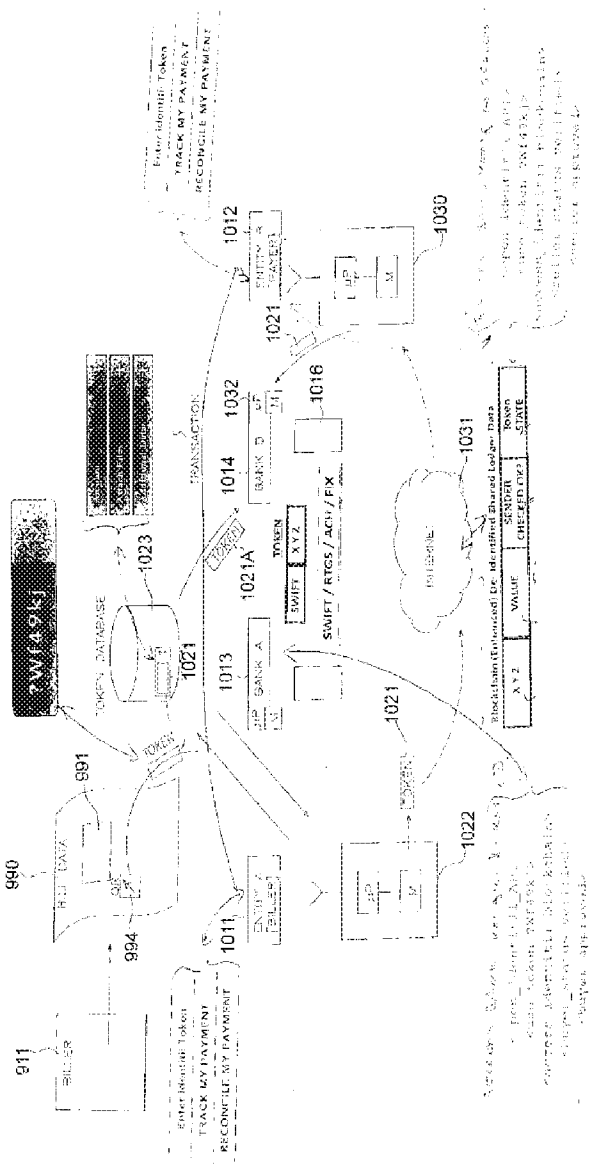

911
990
991
994
1011
1012
1013
1014
1016
1021
1021A
1022
1023
1030
1031
1032
SWIFT / RTGS / ACH / FIX
SWIFT
XYZ
TOKEN
VALUE
SENDER
Token
STATE

FIG. 17

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	Atty. Ref.: AMK-5243-0009
ARMSTRONG et al.	Confirmation No. To Be Assigned
Appln. No. To Be Assigned	Art Unit: To be Assigned
Filed: Concurrently Herewith	Examiner: To be Assigned

For: COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR

* * * * * * * * * * *

February 14, 2018

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

PRELIMINARY AMENDMENT

In order to place the above-identified application in better condition for examination, please amend the application as follows:

AMENDMENTS TO THE ABSTRACT:

Please insert the Abstract of the Disclosure submitted herewith on a separate sheet.

AMENDMENTS TO THE SPECIFICATION:

Page 1, after the title insert the following:

This application is the U.S. national phase of International Application No. PCT/AU2016/000279 filed August 12, 2016 which designated the U.S. and claims priority to Australian Patent Application No. 2015903292 filed August 14, 2015, Australian Patent Application No. 2016900239 filed January 27, 2016, and Australian Patent Application No. 2016901924 filed May 20, 2016, the entire contents of each of which are hereby incorporated by reference.

AMENDMENTS TO THE CLAIMS:

Please cancel claims 1-58 without prejudice or disclaimer.

This listing of claims will replace all prior versions, and listings, of claims in the application:

59. (New) A computer implemented method for processing a financial transaction, the method comprising the steps of:

transmitting one or more documents pertaining to the financial transaction, from a first intermediary server in a centralised financial system to a first document store;

generating an enriched data record from the one or more documents, at the first intermediary server, and adding the enriched data record into a blockchain being a distributed ledger, from the first intermediary sever;

requesting generation of a token corresponding to the financial transaction to identify the one or more documents, to a token server, from the first intermediary server, via a messaging bus in the centralised financial system;

generating the token at the token server and adding the token into the blockchain from the token server in association with the enriched data record;

transmitting the token to the first intermediary server from the token server, via the messaging bus; and

transmitting the token from the first intermediary server to the first document store in association with the one or more documents.

60. (New) The computer implemented method as claimed in claim 59, further comprising the step of sending a first financial message comprising the token, from the first intermediary server to a second intermediary server in the centralised financial system, indicative of making a payment to a second user.

61. (New) The computer implemented method as claimed in claim 59, further comprising the steps of:

implementing a smart contract at the token server; and

adding the smart contract into the blockchain, from the token server.

62. (New) The computer implemented method as claimed in claim 59, further comprising the steps of:

transmitting the token from the first intermediary server to a first digital device available with a first user;

providing the token to a second user, by the first user;

providing the token to a second intermediary server in the centralised financial system, from the second digital device;

transmitting the token to a second document store, from the second intermediary server; and

sending a second financial message comprising the token, from the second intermediary server to the first intermediary server, indicative of making a payment to the first user.

63. (New) The computer implemented method as claimed in claim 59, wherein the step of generating the enriched data record comprises:

extracting a plurality of attributes from the one or more documents, at the first intermediary server; and

combining the plurality of attributes to generate the enriched data record, at the first intermediary server.

64. (New) The computer implemented method as claimed in claim 59, wherein the step of generating the enriched data record comprises:

extracting a plurality of attributes from the one or more documents, at the first intermediary server;

de-identifying the plurality of attributes to obtain a plurality of de-identified attributes, at the first intermediary server; and

combining the plurality of de-identified attributes to generate the enriched data record, at the first intermediary server.

65. (New) The computer implemented method as claimed in claim 59, wherein the step of generating the enriched data record comprises:

extracting a plurality of attributes from the one or more documents, at the first intermediary server;

hashing the plurality of attributes to generate a plurality of respective hashes, at the first intermediary server; and

combining the plurality of hashes to generate the enriched data record, at the first intermediary server.

66. (New) The computer implemented method as claimed in claim 59, further comprising the steps of:

transmitting one or more first requests, each comprising the token, from the first intermediary server to a second intermediary server in the centralised financial system, via the messaging bus;

receiving the one or more first requests at the second intermediary server and transmitting the one or more first requests and the token from the second intermediary server to a second document store;

generating one or more first responses, each comprising the token, corresponding to the respective one or more first requests, at the second intermediary server;

transmitting the one or more first responses from the second intermediary server to the first intermediary server, via the messaging bus;

hashing the one or more first requests and the one or more first responses at the second intermediary server to generate one or more first request hashes and one or more first response hashes, respectively;

adding the one or more first request hashes and the one or more first response hashes to the enriched data record in the blockchain, from the second intermediary server; and

receiving the one or more first responses at the first intermediary server and transmitting the one or more first responses to the first document store.

67. (New) The computer implemented method as claimed in claim 66, further comprising the steps of:

hashing the one or more first responses at the first intermediary server to regenerate the one or more first response hashes; and

verifying the one or more first response hashes with the blockchain from the first intermediary server, using the token.

68. (New) The computer implemented method as claimed in claim 66, wherein each one of the one or more first requests are:

encrypted with a second public key and signed with a first public key at the first intermediary server, before transmission to the second intermediary server; and

decrypted with a second private key at the second intermediary server after reception from the first intermediary server; and

wherein each one of the one or more first responses are:

encrypted with the first public key and signed with the second public key at the second intermediary server, before transmission to the first intermediary server; and

decrypted with a first private key at the first intermediary server after reception from the second intermediary server.

69. (New) The computer implemented method as claimed in claim 59, further comprising the steps of:

transmitting one or more second requests, each comprising the token, from a second intermediary server in the centralised financial system to the first intermediary server, via the messaging bus;

receiving the one or more second requests at the first intermediary server and transmitting the one or more second requests from the first intermediary server to the first document store;

generating one or more second responses, each comprising the token, corresponding to the respective one or more second requests, at the first intermediary server;

transmitting the one or more second responses from the first intermediary server to the second intermediary server, via the messaging bus;

hashing the one or more second requests and the one or more second responses at the first intermediary server to generate one or more second request hashes and one or more second response hashes, respectively;

adding the one or more second request hashes and the one or more second response hashes to the enriched data record in the blockchain, from the first intermediary server; and

receiving the one or more second responses at the second intermediary server and transmitting the one or more second responses to the second document store.

70. (New) The computer implemented method as claimed in claim 69, further comprising the steps of:

hashing the one or more second responses at the second intermediary server to regenerate the one or more second response hashes; and

verifying the one or more second response hashes with the blockchain from the second intermediary server, using the token.

71. (New) The computer implemented method as claimed in claim 69, wherein each one of the one or more second requests are:

encrypted with a first public key and signed with a second public key at the second intermediary server, before transmission to the first intermediary server; and

decrypted with a first private key at the first intermediary server after reception from the second intermediary server; and

wherein each one of the one or more second responses are:

encrypted with the second public key and signed with the first public key at the first intermediary server, before transmission to the second intermediary server; and

decrypted with a second private key at the second intermediary server after reception from the first intermediary server.

72. (New) The computer implemented method as claimed in claim 68, further comprising the steps of adding the first public key from the first intermediary server into the blockchain and adding the second public key from the second intermediary server into the blockchain.

73. (New) A system for processing a financial transaction, the system comprising:

a first intermediary server in a centralised financial system, the first intermediary server being operably connected to a network and a first document store;

a token server operably connected to the network;

a messaging bus in the centralised financial system, the messaging bus being operably connected to the network; and

a blockchain operably connected to the network, the blockchain being a distributed ledger;

wherein the first intermediary server is configured to:

transmit one or more documents pertaining to the financial transaction, to the first document store;

generate an enriched data record from the one or more documents and add the enriched data record into the blockchain;

request generation of a token corresponding to the financial transaction to identify the one or more documents, to the token server, via the messaging bus; and

transmit the token to the first document store;

wherein the token server is configured to:

generate the token and add the token into the blockchain in association with the enriched data record; and

transmit the token to the first intermediary server, via the messaging bus.

74. (New) A first intermediary server for use in a centralised financial system to facilitate processing of a financial transaction, operably connected to a network and a first document store, and configured to:

transmit one or more documents pertaining to the financial transaction, to the first document store;

generate an enriched data record from the one or more documents and add the enriched data record into a blockchain being a distributed ledger;

request generation of a token corresponding to the financial transaction to identify the one or more documents, to a token server, via a messaging bus in the centralised financial system; and

transmit the token to the first document store.

75. (New) The first intermediary server as claimed in claim 74, further configured to send a first financial message comprising the token, to a second intermediary server in the centralised financial system, indicative of making a payment to a second user.

76. (New) The first intermediary server as claimed in claim 74, further configured to transmit the token to a first digital device.

77. (New) The first intermediary server as claimed in claim 74, further configured to:

transmit one or more first requests, each comprising the token, to a second intermediary server in the centralised financial system, via the messaging bus; and

receive one or more first responses from the second intermediary server and transmit the one or more first responses to the first document store.

78. (New) The first intermediary server as claimed in claim 77, wherein the one or more first responses comprise one or more second regulatory compliance documents pertaining to a second user.

REMARKS/ARGUMENTS

Claims 59-78 are present in this application. By this Preliminary Amendment, an Abstract of the Disclosure has been added, the specification has been amended, claims 1-58 have been canceled, and claims 59-78 have been added.

Prompt and favorable examination is respectfully requested.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: /Alan M. Kagen/
Alan M. Kagen
Reg. No. 36,178

AMK:jls
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100

JPMC Ex. 1002
Page 631

ABSTRACT OF THE DISCLOSURE

A computer implemented method for processing a financial transaction includes the steps of transmitting one or more documents pertaining to the financial transaction, from a first intermediary server to a first document store, generating an enriched data record from the one or more documents, at the first intermediary server, and adding the enriched data record into a blockchain, from the first intermediary sever, requesting generation of a token corresponding to the financial transaction, to a token server, from the first intermediary server, via a messaging bus, generating the token at the token server and adding the token into the blockchain from the token server, transmitting the token to the first intermediary server from the token server, via the messaging bus, and transmitting the token from the first intermediary server to the first document store.

JPMC Ex. 1002
Page 632

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 843 587 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
04.03.2015 Bulletin 2015/10

(51) Int Cl.:
G06F 21/64 *(2013.01)*

(21) Application number: **13181902.1**

(22) Date of filing: **27.08.2013**

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME

(71) Applicant: **OpenLimit SignCubes AG**
6341 Baar (CH)

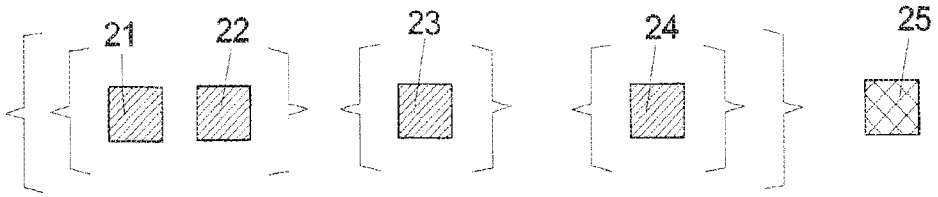
(72) Inventor: **The designation of the inventor has not yet been filed**

(74) Representative: **Gross, Felix et al**
Patentanwälte Maikowski & Ninnemann
Postfach 15 09 20
10671 Berlin (DE)

(54) Method for generating evidence-data for a long-term data storage system for datasets

(57) Method for generating evidence-data for a long-term storage system for datasets (1, 2, 3) being coupled with at least one evidence-data dataset (30) with at least one time stamp dataset (25), wherein
a) for the at least one evidence-data dataset (30) at least one reduced hash-tree dataset is computed with an a priori defined procedure, e.g. according to RFC 4998 or RFC 6283,
b) the at least one evidence-data dataset (30) together with the coupled at least one reduced hash-tree dataset is stored in a first memory means, in particular an archive.

FIG 2



EP 2 843 587 A1

JPMC Ex. 1002
Page 633

Description

[0001] The invention is concerned with a method for generating a long-term data storage system for datasets with the features of claim 1.

[0002] It is a frequent problem to ensure the validity of datasets which need to be stored for a long time. In case e.g. a cryptographic method is found to be unreliable or broken, all respective evidence-data for the datasets need to be updated. Therefore, efficient updating mechanisms are required.

[0003] The generation of the evidence-data can be performed with Merkle hash-trees as described in RFC 4998 (ASN.1 encoding) and RFC 6283 (XML encoding). The direct storage of hash-trees is not described and therefore the implementation varies between manufacturers.

[0004] The method with the features of claim 1 makes the handling of evidence more efficient.

[0005] For the generation of evidence-data for a long-term data storage system datasets are being coupled with at least one evidence-dataset with at least one time stamp dataset, wherein

a) for the at least one evidence-dataset at least one reduced hash-tree dataset is computed with an á priori defined procedure, e.g. according to RFC 4998 or RFC 6283,

b) the at least one evidence-dataset together with the coupled at least one reduced hash-tree dataset is stored in a first memory means, in particular an archive.

[0006] It is part of the invention to use evidence-record datasets as described in the RFCs mentioned above for large archives to store the evidence-data. It is part of the invention to use algorithms that make the handling of the evidence-data in a large archive efficient.

[0007] The invention simplifies the migration of large data covered by evidence-record datasets from one application to another since the evidence-record dataset is stored in a well-defined way through RFC 4998 or RFC 6283. These RFCs might at one point in time be replaced or updated by other equivalent definitions. It is important that the evidence record is clearly defined á priori, not necessarily by the RFC 4998 or RFC 6283.

[0008] Some embodiments are shown in the following Figures.

Fig. 1 showing a Merkle hash-tree for some datasets;

Fig. 2 a reduced hash-tree for the example given in Fig. 1;

Fig. 3 a reduced hash-tree with a link;

Fig. 4 a reduced hash-tree with a link and a revocation information;

Fig. 5 a hash-tree with a renewed time stamp;

Fig. 6 a renewed reduced hash-tree.

[0009] Before describing some embodiments, the meaning of certain terms is described.

[0010] A long-term data storage system for datasets is to be understood as an archive. The evidence-record datasets 30, e.g. according to the RFC 4998 or RFC 6268 are generated in a way that the integrity of the data can be proven or validated.

[0011] A time stamp dataset is a time stamp without an explicitly mentioned RFC.

[0012] A revocation dataset is a revocation information without an explicit mentioning of an RFC or certain data structures. Fig. 1 shows schematically a Merkle hash-tree with coupled datasets 1, 2, 3 and other datasets; the datasets themselves do not belong to the hash-tree.

[0013] On top of the hash-tree is a time-stamp dataset 25. The valid signature of the time-stamp dataset 25 guarantees the integrity of all associated datasets as long as the hash-and the signature algorithm is strong. The datasets 1, 2, 3 typically comprise information which require a long-term storage, e.g. land register records or patent documents. The long-term storage can be determined by legal provisions and can last e.g. for 3 or more than 10 years or even indefinitely.

[0014] For each of the datasets 1, 2, 3 hash-datasets 21, 22 are generated and a hash-tree with intermediate hash-datasets 23, 24 is generated. Intermediate hash-datasets 23, 24 allow for an increased flexibility in the ordering of hash value computations. For the top of the tree a time stamp dataset 25 is generated.

[0015] The time-stamp dataset 25 applies to all hash-datasets 21, 22, 23, 24 in the tree structure.

[0016] The storage of hash-trees as evidence-data for long-time storage is currently proprietary and might be error prone since one error in the structure might affect all coupled datasets 1, 2, 3. Migration of evidence-records from one application to another is robust, i.e. the data integrity is strong, because the data structures are well defined and every two distinct evidence-records are independent.

[0017] Part of the method described herein is the immediate generation of the evidence-data (see Fig. 2) specifically for every dataset 1, 2, 3. This evidence-data could be an evidence-record dataset 30 as defined by RFC 4998 or RFC 6283 or other data which prove the validity of the dataset. An evidence-record dataset 30 as defined by the respective RFCs is well known by every application supporting the respective RFC. Since the RFCs are widely accepted and an evidence-record dataset 30 is well-defined this dataset is suited for long-term storage.

[0018] The generation of evidence-record datasets 30 from hash-trees like the one shown in Fig. 1 is described schematically in Fig. 2.

[0019] The hash-datasets 21, 22, 23, 24 are stored in a list of lists. Hash-datasets 21, 22, 23, 24 from the same

JPMC Ex. 1002
Page 634

level of the tree share one list each. The first list in the inner level comprises two hash-datasets 21, 22. On the same level two more lists comprise one dataset 23, 24 each.

[0020] The hash-datasets 21, 22, 23, 24 together with the time-stamp dataset 25 form a reduced hash-tree as described in the respective RFCs. A reduced hash-tree contains the minimum of hash-datasets to be able to validate the top-most hash-dataset stored in the time-stamp dataset 25.In the example of Fig. 1 the hash-datasets 21, 22 in the first sequence represent the documents 2, 3.

[0021] Together with the intermediate hash-datasets 23, 24 and the time-stamp dataset 25 they form a reduced hash-tree. This reduced hash-tree comprises the schematically evidence-record dataset 30.

[0022] The reduced hash-tree shown in Fig. 2 relates to the documents 2, 3. The further intermediate hashes 23, 24 are chosen so that the computation of the hash value at the top of the hash tree is possible, subject to the condition that a minimal number of hashes need to be included into the evidence records dataset or reduced hash tree, as stipulated by the RFCs.

[0023] The evidence-record dataset 30 is therefore well-defined and this makes it easy to migrate the data from one application to another.

[0024] An error in the structure of an evidence-record dataset 30 per dataset affects only the coupled dataset 2, 3 and therefore, the embodiment of the invention stabilizes the long-time storage of evidence-record datasets 30 against failure. If in the future the mechanisms to store datasets 1, 2, 3 are changed, the dataset "evidence-record" 30 will not be affected because the data structure is well-defined. This means that structure of the evidence-record dataset is defined down to the bit level. This is in contrast to hash trees e.g. as SQL-Text, XML-Text, proprietary MySQL or in an Oracle-database.

[0025] In one embodiment of the invention - schematically depicted in Fig. 3 - an option to store the time-stamp dataset 25 separate from the evidence-record dataset 30 via a link 26 from the evidence-record dataset 30 to the time-stamp dataset 25 exists. In this case the time-stamp data set 25 belongs to the RFC evidence record structure. With the mere reference to the time-stamp dataset 25 the well define RFC conform evidence record is altered and comprises a proprietary part. But the advantage is gained that the one-time reference on the time-stamp dataset 25 is easier to process than a previous, more complex hash-tree.

[0026] The linkage of the time-stamp dataset 25 can reduce duplication of data since the time-stamp dataset 25 is stored only once.

[0027] From time to time the evidence-data needs refresh to stay current. Typically the following actions are performed:

1) Adding of a revocation dataset to evidence-data.

2) Renewal of time stamp dataset.

3) Renewal of hash-algorithm.

[0028] In general, these actions are defined in RFC 4998 and RFC 6283. In the following these actions will be described in more detail for the application to the invention.

[0029] Ad 1) Adding of a revocation dataset to evidence-data.

[0030] The addition of a revocation dataset 28 to evidence-data ensures the revocation dataset 28 is present if it is needed for verification purposes.

[0031] In one embodiment of the invention the gathering of the revocation dataset 28 of the duplicated time stamp datasets must only be done once for each duplicated time stamp dataset. Therefore, the incorporation of the revocation dataset 28 into the time stamp data dataset might duplicate data but the gathering of the revocation dataset could be done once and is therefore efficient.

[0032] In another embodiment the revocation dataset 28 could be stored apart from the time stamp dataset 25 with only a link to the revocation dataset 28.

[0033] This can reduce the duplication of data if duplicated data is stored only once. For clarity, the situation with linked time stamp dataset 25 and linked revocation dataset 28 is shown in Fig. 4.

[0034] Ad 2) Renewal of time stamp dataset.

[0035] From time to time there is a need to renew the time stamp dataset 25. One reason for this can be the relative weakness of the cryptographic signature of the time stamp dataset 25. The renewal of the time stamp dataset 25 comprises the adding of new evidence-data with a fresh time stamp dataset 25. The fresh evidence-data is built from the previous time stamp dataset 25.

[0036] It is part of the invention that renewal of time stamp dataset 25 of the duplicated time stamp datasets must only be done once for each duplicated time stamp dataset 25. Therefore, renewal of time stamp datasets is efficient.

[0037] For clarity, Fig. 5 shows renewal of time stamp datasets 41, 42 with a newly generated intermediate hash-tree. On top of the newly generated hash-tree is a fresh time-stamp dataset 45. Below the time stamp datasets 41, 42 it is shown the virtual reconstruction of the former hash-trees which have time-stamp datasets 41 and 42 on top as described in the respective RFC's.

[0038] It is part of the invention that the virtual reconstruction of the former hash-trees work efficient with reduced hash-trees for time-stamp renewal.

[0039] This is a kind of virtual reconstruction of a hash tree. Indeed a time stamp dataset 25 - which might be stored multiple times in an archive - is only used once for the renewal of the time stamp dataset 25.

[0040] Fig. 6 schematically shows the new reduced hash-tree 41, 42, 43 and the time-stamp dataset 45 concatenated to the previous evidence-data. For the sake of clarity optional linkage of time stamp dataset and revocation dataset is omitted. In one embodiment the tem-

JPMC Ex. 1002
Page 635

porarily built hash-tree is immediately reduced and the evidence-data is stored per dataset. In a further embodiment the time stamp dataset is stored apart from basic evidence-data with a link from evidence-data to time stamp dataset. This can reduce the duplication of data since the time stamp dataset and / or the revocation dataset is stored only once.

[0041] Ad 3) Renewal of hash-algorithm.

[0042] From time to time there is a need to renew the used hash-algorithm. One reason for this could be the relative cryptographic weakness of the used hash-algorithm.

[0043] In general, the renewal of the hash-algorithm enforces the generation of evidence-data per dataset as it is described in RFC 4998 or RFC 6283. Part of the invention is the immediate generation of evidence-data per dataset so this step is efficient.

[0044] For large long-term data storage systems the invention obsoletes the storage of hash-trees as evidence-data. The invention favors to store evidence-data per dataset. The evidence-data per dataset could be an evidence-record dataset 30 as described in RFC 4998 or RFC 6283, or - to reduce time-stamp dataset duplication or revocation dataset duplication - a structure which consists of reduced hash-tree(s) and link(s) to stored apart time stamp datasets and revocation datasets. To accomplish this, temporarily built hash-trees are reduced immediately after building.

[0045] The invention is efficient for the steps of gathering revocation information, renewal of time stamp dataset and renewal of hash-algorithm. The invention let duplicate data (e.g. time stamp datasets and revocation datasets) but the invention has the option to store time stamp datasets and revocation datasets apart from the base evidence-data which can reduce the duplication.

[0046] For the purpose of this description, the term "evidence-data dataset" implies that the integrity of a coupled dataset can be proven. Evidence-records as defined in the respective RFCs are examples of "evidence-data". A hash-tree is an other example of evidence-data.

Reference Numbers

[0047]

1 dataset
2 dataset
3 dataset

21 hash-dataset
22 hash-dataset
23 hash-dataset
24 hash-dataset
25 timestamp-dataset
26 link
27 link
28 revocation dataset
30 evidence-record dataset

41 hash-dataset
42 hash-dataset
43 hash-dataset
45 timestamp-dataset

Claims

1. Method for generating evidence-data for a long-term storage system for datasets (1, 2, 3) being coupled with at least one evidence-data dataset (30) with at least one time stamp dataset (25), wherein

   a) for the at least one evidence-data dataset (30) at least one reduced hash-tree dataset is computed with an á priori defined procedure, e.g. according to RFC 4998 or RFC 6283,
   b) the at least one evidence-data dataset (30) together with the coupled at least one reduced hash-tree dataset is stored in a first memory means, in particular an archive.

2. Method according to claim 1, wherein during a renewal of the at least one evidence-data dataset (30) at least one new evidence-data dataset is generated from the previous at least one evidence-data dataset (30) by generating at least one new time stamp dataset (45), in particular by augmenting the previous evidence-data dataset (30).

3. Method according to claim 1 or 2, wherein the hash-algorithm for generating the at least one reduced hash-tree dataset is renewed by accessing the already stored at least one evidence-data dataset (30) and the at least one new evidence-data record is augmented with the newly generated at least one reduced hash-tree dataset.

4. Method according to at least one of the preceding claims, wherein the at least one evidence-data dataset (30) is coupled with at least one time stamp dataset (25).

5. Method according to at least one of the preceding claims, wherein the at least one time stamp dataset (25, 45) is coupled at least to one revocation dataset (28).

6. Method according to at least one of the preceding claims, wherein for the at least one evidence-data dataset (30) the at least one time stamp dataset (25) is replaced by a time stamp dataset pointer (26) and the new time stamp dataset is stored in a second memory means.

7. Method according to at least one of the preceding

JPMC Ex. 1002
Page 636

claims, wherein for the at least one evidence-data dataset (30) and / or the at least one time stamp dataset (25) the at least one revocation dataset (28) is replaced by a revocation dataset pointer (27) and the at least one revocation dataset (28) is stored in a third memory means.

8. Method according to at least one of the preceding claims, wherein the renewal of the at least one time stamp (25) and / or the at least one revocation dataset (28) is performed only on evidence-data datasets (30) with identical time stamp datasets (25).

9. Method according to at least one of the preceding claims, wherein the at least one evidence-data dataset (30) comprises an XML structure according to RFC 6283 or a binary structure according to RFC 4998.

JPMC Ex. 1002
Page 637

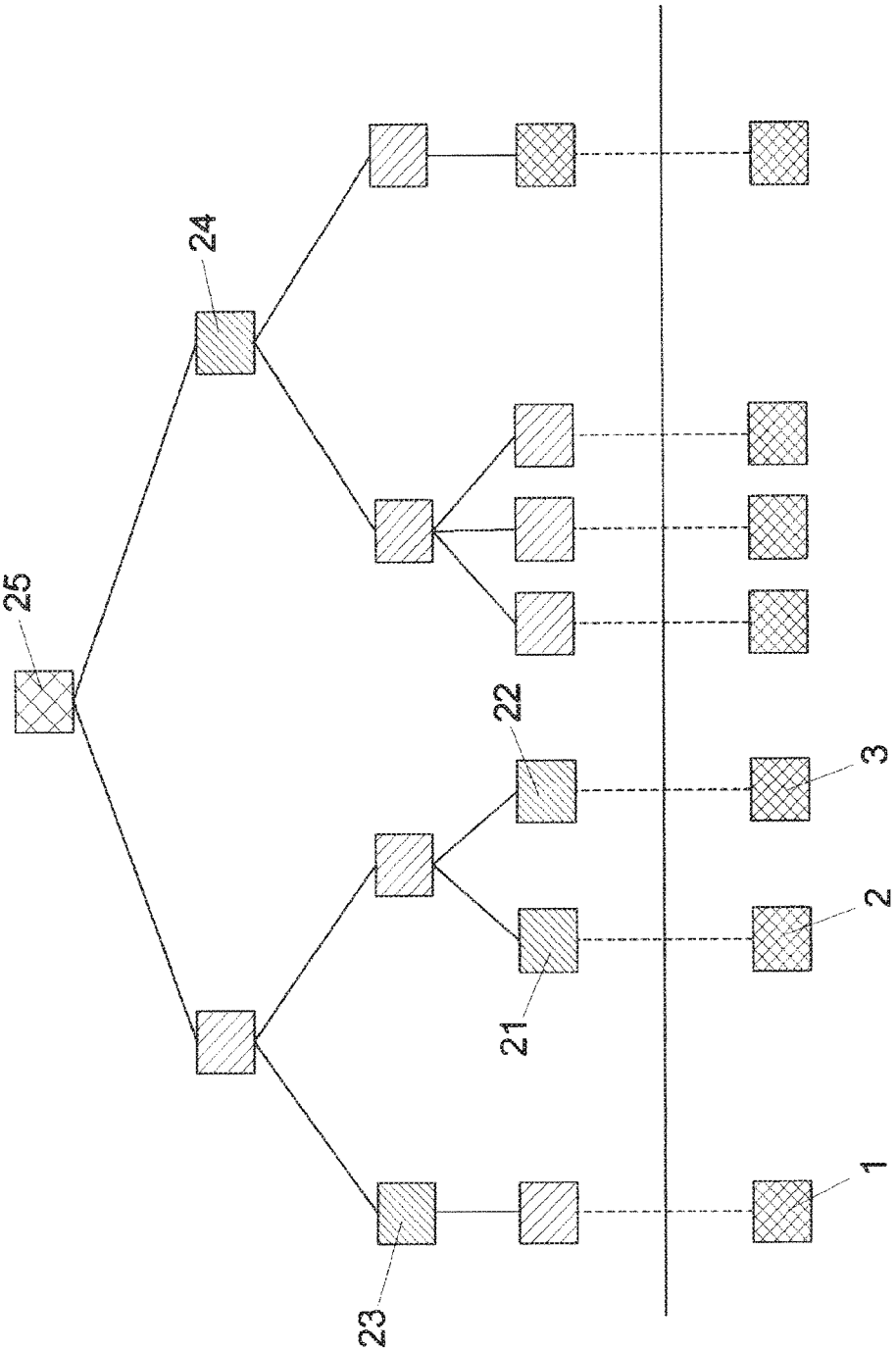


FIG 1

JPMC Ex. 1002
Page 638

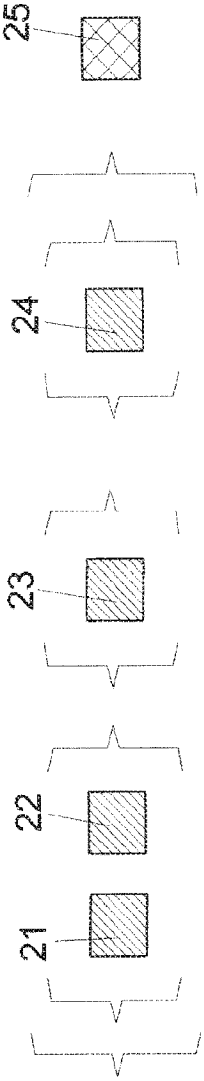


FIG 2

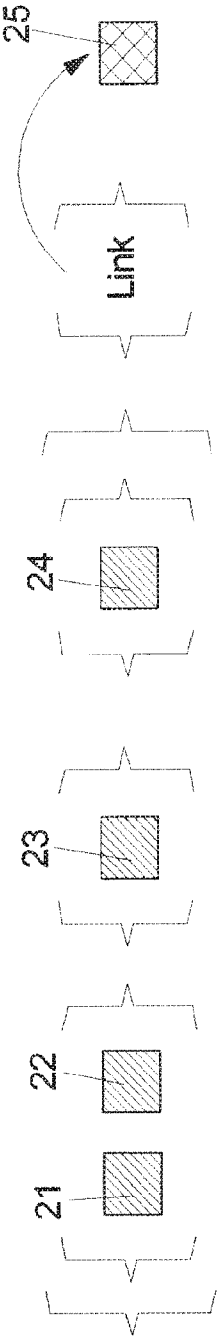


FIG 3

JPMC Ex. 1002
Page 639

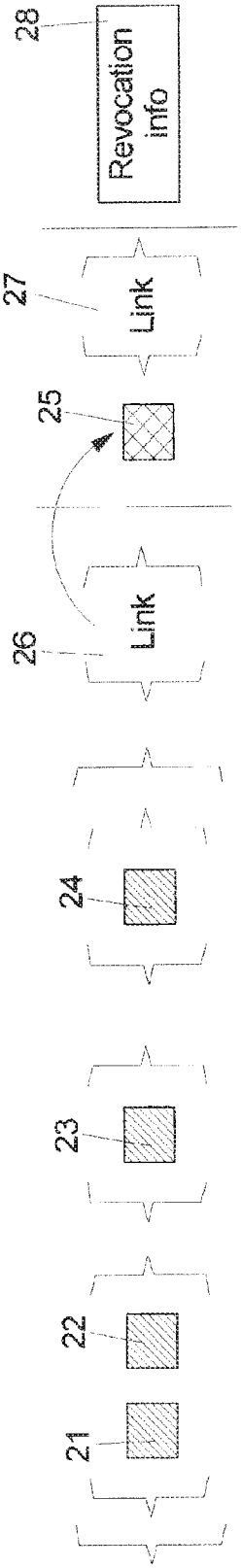


FIG 4

JPMC Ex. 1002
Page 640

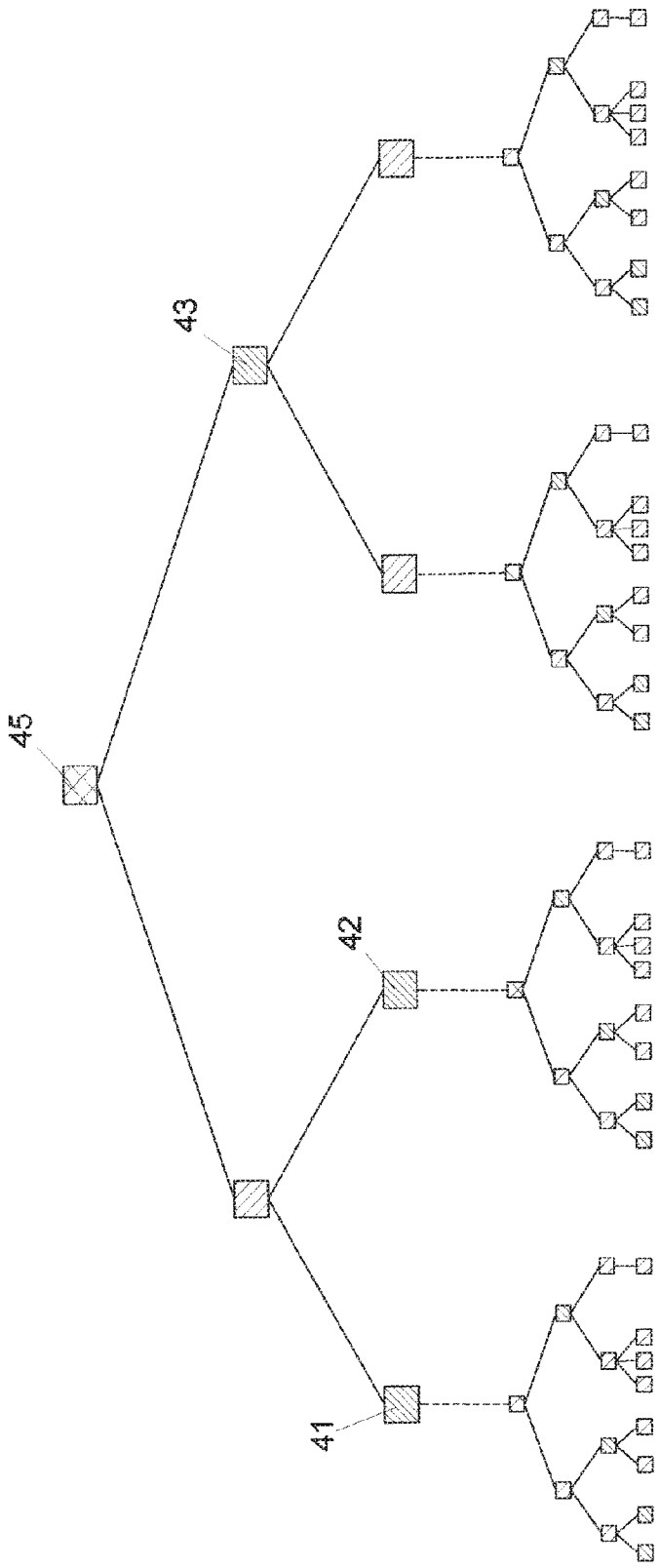
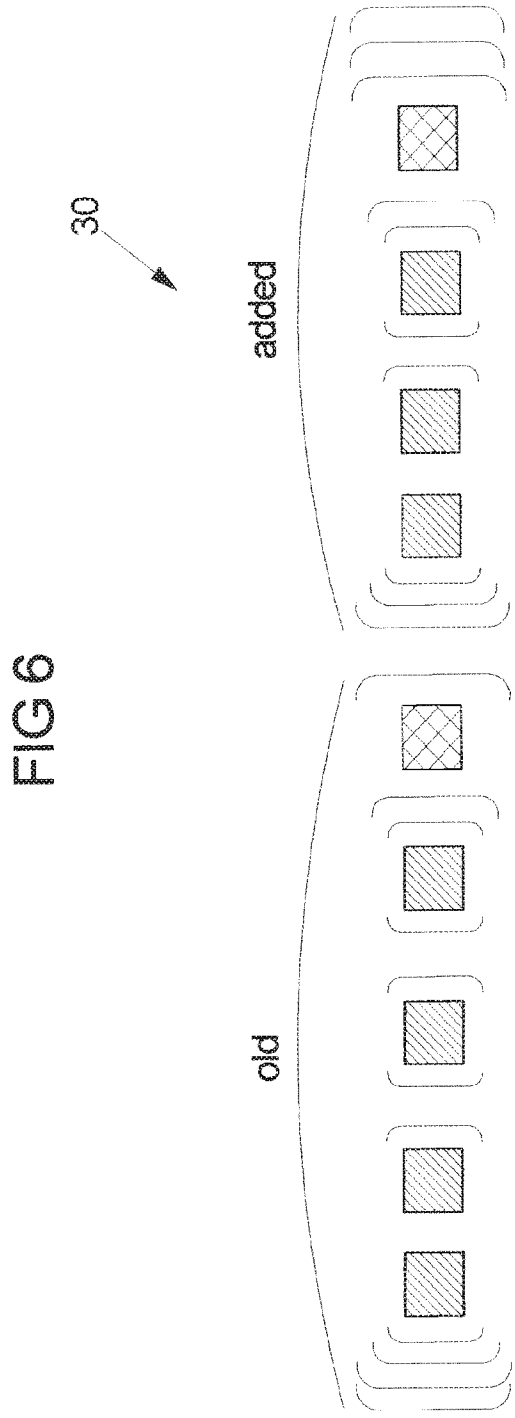


FIG 5

JPMC Ex. 1002
Page 641

FIG 6



JPMC Ex. 1002
Page 642

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 13 18 1902

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	T Gondrom ET AL: "Network Working Group", , 31 August 2007 (2007-08-31), page 1997, XP055108957, Retrieved from the Internet: URL:http://tools.ietf.org/pdf/rfc4998.pdf [retrieved on 2014-03-19]	1-8	INV. G06F21/64
Y	* the whole document *	9	
Y	A Jerman Blazic: "RFC 6283 - Extensible Markup Language Evidence Record Syntax (XMLERS)", , 30 July 2011 (2011-07-30), XP055109278, Retrieved from the Internet: URL:http://www.rfc-editor.org/rfc/pdfrfc/rfc6283.txt.pdf [retrieved on 2014-03-21] * the whole document *	9	
A	WO 2006/066142 A2 (NTT DOCOMO INC [JP]; RAMZAN ZULFIKAR AMIN [US]; GENTRY CRAIG B [US]; B) 22 June 2006 (2006-06-22) * the whole document *	1	TECHNICAL FIELDS SEARCHED (IPC) G06F
A	HYLA T ET AL: "Long-term preservation of digital signatures for multiple groups of related documents", IET INFORMATION SECURITY, THE INSTITUTION OF ENGINEERING AND TECHNOLOGY, MICHAEL FARADAY HOUSE, SIX HILLS WAY, STEVENAGE, HERTS. SG1 2AY, UK, vol. 6, no. 3, 10 September 2012 (2012-09-10), pages 219-227, XP006043033, ISSN: 1751-8709, DOI: 10.1049/IET-IFS.2011.0344 * the whole document *	1	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	21 March 2014	Yanai, Yoav

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

JPMC Ex. 1002
Page 643

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 13 18 1902

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

21-03-2014

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2006066142 A2	22-06-2006	EP 1825377 A2	29-08-2007
		JP 2008524930 A	10-07-2008
		US 2006137006 A1	22-06-2006
		US 2006242699 A1	26-10-2006
		US 2006248334 A1	02-11-2006
		US 2010153714 A1	17-06-2010
		US 2010174904 A1	08-07-2010
		WO 2006066142 A2	22-06-2006

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

JPMC Ex. 1002
Page 644

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 August 2015 (06.08.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/116998 A2

(51) International Patent Classification:
G06Q 40/06 (2012.01)

(21) International Application Number:
PCT/US2015/013908

(22) International Filing Date:
30 January 2015 (30.01.2015)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/933,474 30 January 2014 (30.01.2014) US

(72) Inventor; and
(71) Applicant : **KREMEN, Gary** [US/US]; 1259 El Camino Real, #500, Menlo Park, California 94025 (US).

(74) Agents: **CHENG, Shih-Yo (Shawn)** et al.; Perkins Coie LLP, P. O. Box 1208, Seattle, Washington 98111-1208 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

---- *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

(54) **Title**: ELECTRONIC TRANSFER AND OBLIGATION ENFORCEMENT SYSTEM

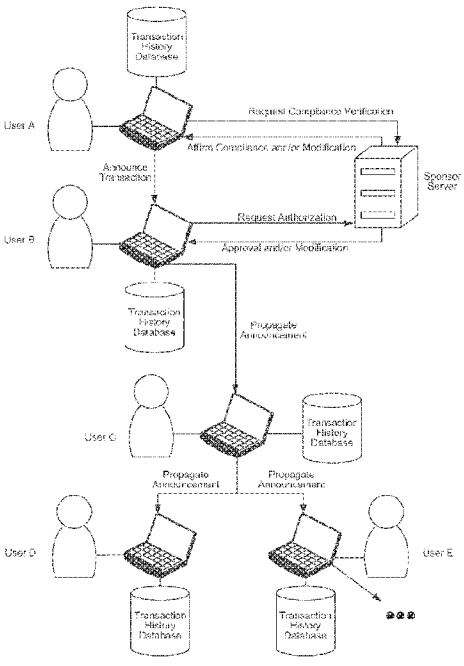


FIG. 2

(57) **Abstract**: Several embodiments includes a secured method of implementing an electronic transfer system in a distributed manner while enforcing an obligatory distribution rule. A computer can receive an electronic record representing an electronic transfer of a transfer amount from a source account to a destination account; verify availability of the transfer amount from the source account via a public ledger in a distributed consensus system; determine a conditional circumstance of the electronic transfer; access an obligatory distribution rule object, wherein the obligatory distribution rule object dictates how the transfer amount is distributed amongst the destination account and at least a third account; authenticate the obligatory distribution rule object with a sponsor server; and generate a second electronic record based on the obligatory distribution rule object, the conditional circumstance, and/or the electronic record to modify the electronic transfer to distribute a portion of the transfer amount to the third account.

WO 2015/116998 A2

ELECTRONIC TRANSFER AND OBLIGATION ENFORCEMENT SYSTEM

CROSS-REFERENCE TO RELATED APPLICATION(S)

[0001] This application claims the benefit of U.S. Provisional Patent Application No. 61/933,474, entitled "ELECTRONIC TRANSFER AND OBLIGATION ENFORCEMENT SYSTEM," which was filed on January 30, 2014, which is incorporated by reference herein in its entirety.

RELATED FIELD

[0002] This disclosure relates to electronic transfer systems. More particularly, this disclosure relates to systems and techniques for implementing a decentralized electronic transfer system.

BACKGROUND

[0003] Decentralized electronic transfer systems are created to circumvent the necessity and avoid the costs of having a central entity checking and validating each transfer. Central electronic transfer systems rely on the central entity to validate a transfer request made by a user via identification and authentication of the user. An electronic transfer represents a persistent record of an electronic communication that denotes a public or semi-public transfer of quantified value from one account to another.

[0004] On the other hand, decentralized electronic transfer systems rely on identification and publication of user accounts (e.g., via public electronic addresses whose ownership is cryptographically verifiable) and electronic transfers to validate a transfer request. This enables the public to access all electronic transfers in a public ledger (e.g., maintained in a distributed consensus system) and to check the correctness (e.g., via cryptographic verification) of such electronic transfers in these decentralized systems. This form of crowd-based transfer control, combined with mechanisms to reject incorrect published transfers, form the backbone of most decentralized electronic transfer systems. The decentralized electronic transfer systems enable users to remain anonymous in each transfer.

[0005] A drawback of the decentralized electronic transfer system is a lack of means to enforce legal obligations that is normally associated with other electronic transfers. Consequently, use of decentralized electronic transfer systems can become a channel to avoid legal obligations.

JPMC Ex. 1002
Page 646

Brief Description of the Drawings

[0006] **FIG. 1** is a diagrammatic representation of a conventional decentralized digital exchange system.

[0007] **FIG. 2** is a diagram illustrating a decentralized electronic transfer system with distribution control capability.

[0008] **FIG. 3** is an example of a data flow diagram for initiating an electronic transfer on the electronic transfer system.

[0009] **FIG. 4** is a control flow diagram of an electronic transfer system for facilitating secure electronic transfers.

[0010] **FIG. 5** is a flow chart of a method of operating a computing node in an electronic transfer system for facilitating secure electronic transfers.

[0011] **FIG. 6** is a diagrammatic representation of a machine in the exemplary form of a computer system within which a set of instructions, for causing the machine to perform any one or more of the methodologies or modules discussed herein, may be executed.

[0012] The figures depict various embodiments for purposes of illustration only. One skilled in the art will readily recognize from the following discussion that alternative embodiments of the structures and methods illustrated herein may be employed without departing from the principles of the embodiments described herein.

JPMC Ex. 1002
Page 647

Detailed Description

[0013] This disclosure is directed at technical means for authorizing and modifying electronic transfers based at least in part on digital means of determining obligations associated with each electronic transfer. Such obligations may stem from obligations of residents within a governing sovereignty, such as tax obligations within a country. Such obligations may also stem from contractual obligations for using a particular electronic transfer related service, such as crypto-currency service, electronic insurance service, electronic banking service, electronic transaction service, digital accounting service, etc. The disclosed techniques can provide a method of enforcing legal obligations while allowing at least some of the participants of the electronic transfers to remain anonymous. The disclosed techniques further provide a way for a sponsor (*e.g.*, the beneficiary of the obligations) or a hierarchy of sponsors to manage and modify the obligations at a system-level to ensure that all electronic transfers, anonymous or not, are consistent with the obligations.

[0014] An electronic transfer system implementing the disclosed techniques can provide secured publication and authentication of the rules that dictate the obligations of parties in an electronic transfer. The secured publication and authentication of these rules issued by the sponsor(s) protect the electronic transfers against malicious electronic attacks and scams. Once authenticated, the issued rules can become a fundamental part of the electronic transfer system implemented by a network of computing nodes. Alternatively, the issued rules can be inserted into each electronic transfer as part of the digital contract of the electronic transfer. It is hence noted that these technical means are beyond mere administrative procedures that a computer programmer may be asked to implement.

[0015] A decentralized electronic transfer system may include computing nodes that are each capable of identifying, validating, and publishing transfer requests. Each transfer request may require a validation that a source account derives a transfer amount from a history of electronic transfers. The validation serves to verify at least one part of the transfer request. A cryptographic verification of each block in the chain of transfer further validates the transfer request.

[0016] The disclosed electronic transfer system can issue digital currency cryptographically. The electronic transfer system can safeguard the safety, integrity, and balance of all ledgers for the digital currency via cryptographic signatures and proof of work. The disclosed electronic transfer system can enable bond issuance and inflation control of the digital currency. The disclosed electronic transfer system can issue new digital currency from the sponsor and buy back existing digital currency from the sponsor. The disclosed

JPMC Ex. 1002
Page 648

electronic transfer system further enables the sponsor to back the digital currency with real property or physical items, such as precious metal. The disclosed electronic transfer system can maintain audit trails for all electronic transfers so that the sponsor can enforce contractual or legal rules or laws despite granting the ability for participants to be anonymous.

[0017] **FIG. 1** is a diagrammatic representation of a conventional decentralized digital exchange system 100, such as BitCoin or Ripple. The digital exchange system 100 can be implemented by a decentralized network of computing nodes, such as desktop computers, computer servers, mobile devices, or any combination thereof. Computing nodes can freely join the network to request an electronic transfer involving an amount of digital currency or leave the network. Every computing node within the network can store a complete history of all electronic transfers ever made in the digital exchange system 100.

[0018] **FIG. 2** is a diagram illustrating a decentralized electronic transfer system 200 with distribution control capability. The electronic transfer system 200 can also be implemented by a decentralized network of computing nodes. The computing nodes can also freely join the network to request an electronic transfer or leave the network. Every computing node within the network can store a complete history of all electronic transfers ever made in the electronic transfer system 200. The electronic transfer system 200 differs from the conventional digital exchange in that a sponsor or a hierarchy of sponsors can propagate rules to modify all electronic transfers going through the electronic transfer system. These rules can be cryptographically verified so that malicious entities are prevented from destroying or stealing ownership interests of any accounts within the electronic transfer system.

[0019] **FIG. 3** is an example of a data flow diagram for initiating an electronic transfer on the electronic transfer system. Illustrated is a transfer request 302 that can be propagated from computer node to computer node within a decentralized electronic transfer system, such as the electronic transfer system 200 of **FIG. 2**, implemented by a network of computer nodes. The transfer request 302 includes an indication of a source account 304 and an indication of a destination account 306. In some embodiments, the transfer request 302 can include multiple source accounts and/or multiple destination accounts. An indication of the source account 304 can include attributes of the source account, such as location, IP address, or identifier (*e.g.*, via national identification schemes such as Social Security). An indication of the destination account 306 can include attributes of the destination account, such as location, IP address, or identifier (*e.g.*, via national identification schemes such as Social Security). The transfer request 302 further includes an indication of a transfer amount

JPMC Ex. 1002
Page 649

308. Optionally, the transfer request 302 may indicate the currency type(s) of digital or real-world currency to use for the electronic transfer.

[0020] A computing node can verify the transfer amount 308 against a block chain 310 of electronic transfers. The block chain is a sequential linked list of blocks, where each block is a group of electronic transfers that are deemed to have occurred concurrently. The computing node can determine a complete electronic transfer history 311 of all electronic transfers that occurred on the electronic transfer system from the block chain 310.

[0021] The computing node can determine whether the transfer request 302 needs to be modified by checking against an obligatory distribution rule object 312. The obligatory distribution rule object 312 is a data structure that dictates the circumstances under which a transfer request should be modified, how the transfer request should be modified, and how much of the transfer amount is to distribute amongst the destination account and one or more sponsor accounts. The obligatory distribution rule object 312 may be a hierarchical data structure, where the distribution rule corresponding to a higher level node (*i.e.*, closer to the root node) applies first before the distribution rule corresponding to a lower level applies.

[0022] The transfer request 302 may include other electronic transfer information 314, such as timestamp of the request, available currency of the source account, other self-reported information by a user of the source account, an object (*e.g.*, merchandise or services) of the request, contractual terms of the request, necessary conditions to effectuate the electronic transfer, etc., or any combination thereof. All of the information contained within the transfer request 302 may be used to match an entry within the obligatory distribution rule object 312. The entry dictates how the transfer request should be modified and how much of the transfer amount is to distribute amongst the destination account and the one or more sponsor accounts. Optionally, the transfer request 302 may include a sponsor list 316. The user of the source account can voluntarily include itself under the jurisdiction of particular sponsors listed in the sponsor list 316 in exchange for service, legal rights or interest, monetary incentive, property, or a combination thereof.

[0023] **FIG. 4** is a control flow diagram of a computing node 400 of an electronic transfer system, such as the electronic transfer system 200 of **FIG. 2**. The computing node 400 can facilitate secure electronic transfers within the electronic transfer system implemented by network of computing nodes. The computing node 400 includes a user interface module 402. The user interface module 402 generates and displays a user interface so that a user can make electronic transfers through the electronic transfer system. The user

JPMC Ex. 1002
Page 650

interface may request the user to present a private key associated with a user account whenever the user requests an electronic transfer to be made.

[0024] The computing node 400 also includes a transfer protocol module 404 implemented to communicate with other computing nodes within the electronic transfer system. The transfer protocol module 404 may include a cryptography module 406 capable of verifying certificate signatures. The cryptography module 406 can determine a hash code from a message and/or a private key. The cryptography module 406 can also verify whether a given private key matches a given hash code.

[0025] The transfer protocol module 404 has access to a local memory 408. The local memory 408 may include a rule object cache 410 and a transfer history cache 412. The rule object cache 410 stores at least an instance of an obligatory distribution rule object, such as the obligatory distribution rule object 312 of **FIG. 3**. The transfer protocol module 404 can update the rule object cache 410 with a newer instance of the obligatory distribution rule object based on an updated schedule or in response to push messages from one or more sponsor servers (*i.e.*, computing devices operated by one of the sponsor entities). The cryptography module 406 can authenticate such updates. The transfer history cache 412 stores a block chain of electronic transfers, such as the block chain 310 of **FIG. 3**. The transfer protocol module 404 can update the transfer history cache 412 from one or more peer computing nodes in the electronic transfer system. The cryptography module 406 can authenticate each block within the block chain.

[0026] Regarding **FIG. 4**, blocks, components, and/or modules associated with the computing node 400, each may be implemented in the form of special-purpose circuitry, or in the form of one or more appropriately programmed programmable processors, or a combination thereof. For example, the modules described can be implemented as instructions on a tangible storage memory capable of being executed by a processor or a controller on a machine. The tangible storage memory may be volatile or non-volatile memory. In some embodiments, the volatile memory may be considered "non-transitory" in the sense that it is not a transitory signal. Modules may be operable when executed by a processor or other computing device, *e.g.*, a single board chip, application-specific integrated circuit, a field programmable field array, a network capable computing device, a virtual machine terminal device, a cloud-based computing terminal device, or any combination thereof. Caches, memory space, and storages described in the figures can be implemented with the tangible storage memory as well, including volatile or non-volatile memory.

JPMC Ex. 1002
Page 651

[0027] Each of the modules may operate individually and independently of other modules. Some or all of the modules may be executed on the same host device or on separate devices. The separate devices can be coupled via a communication module to coordinate its operations via an interconnect or wirelessly. Some or all of the modules may be combined as one module.

[0028] A single module may also be divided into sub-modules, each sub-module performing separate method step or method steps of the single module. In some embodiments, the modules can share access to a memory space. One module may access data accessed by or transformed by another module. The modules may be considered "coupled" to one another if they share a physical connection or a virtual connection, directly or indirectly, allowing data accessed or modified from one module to be accessed in another module. In some embodiments, some or all of the modules can be upgraded or modified remotely. The computing node 400 may include additional, fewer, or different modules for various applications.

[0029] **FIG. 5** is a flow chart of a method 500 of operating a computing node in an electronic transfer system for facilitating secure electronic transfers. The electronic transfer system can be implemented as a decentralized network of computer nodes. For example, applications on the computer nodes can share a standardized protocol or application programming interface to make electronic transfers. The electronic transfers are transactions that move a quantity of accountable resources from one account to another. The electronic transfers are identified, verified, validated, and published by the network of computing nodes. The accountable resources may include social currency (*e.g.,* social approval rating, social trust score, etc.), electronic records of credit/debit, digital ledgers, digital currency, crypto-currency (*e.g.,* Bitcoin, Novacoin, XRP, Linden dollars), other means of tracking real world or virtual items of value, interest, obligation, rights, or ownership share, or any combination thereof.

[0030] The method 500 includes a computer node receiving, in step 502, a first digital string representing an electronic transfer of a transfer amount from a source account to a destination account. The first digital string represents a transfer request. Step 502 can represent the step where the user of the source account attempts to initiate an electronic transfer to move the transfer amount of accountable resources to the destination account.

[0031] Before publishing the electronic transfer, the electronic transfer system must verify the availability of the transfer amount and determine whether any obligatory distribution has to be made from the transfer amount or whether the transfer amount has to be

JPMC Ex. 1002
Page 652

modified. As shown in **FIG. 5**, a computer node verifies, in step 504, the availability of the transfer amount from the source account via a transaction history. The computer node of step 504 can be the computer node that received the first digital string and publishes the first digital string. The computer node of step 504 can also be a computer node that is propagating the electronic transfer through the decentralized network. Further, the computer node of step 504 can be a block producing computer node that decides whether to include the electronic transfer in a new block that is to be included in the next instance of the transaction history. The transaction history is a chain of blocks. Each block can be cryptographically validated. Each block contains a group of electronic transfers that have been sent since the previous block. The transaction history can be used to validate electronic transfers that traces the transfer amount of accountable resources have indeed been allocated to the source account since the latest block in the transaction history. For example, each block in the chain of verifiable electronic transfers can be verified and validated mathematically through a cryptographic proof of work, such as using a hashcash cost function. Other technical methods known to one of ordinary skill in the related field of this disclosure can also be used to verify the availability of the transfer amount.

[0032] The computer node can also access, in step 506, conditional circumstances of the electronic transfer after the transfer request is received. A conditional circumstance is a digital means of quantifying an attribute of the electronic transfer or of accounts involved in the electronic transfer. The conditional circumstances may be used to determine how the transfer amount is to be distributed to the destination account and/or to at least a third account. In various embodiments, the third account represents a government taxing agency. A conditional circumstance of the electronic transfer may pertain to an attribute of the source account, an attribute of the destination account, an attribute of the electronic transfer, or an attribute of the third account. For example, the conditional circumstance may be an identification (*e.g.,* ID links to national identity schemes such as Social Security numbers) of the source account, the destination account, or the third account. As another example, the conditional circumstance may be a physical or virtual location identifier of the source account, the destination account, or the third account.

[0033] Other examples of the conditional circumstances include a time stamp of the electronic transfer; an account type of the source account, the destination account, or the third account; the transfer amount involved in the electronic transfer; revenue of the source account, the destination account, or the third account; business type of the source account, the destination account, or the third account; a digital indication of an object of the electronic

JPMC Ex. 1002
Page 653

transfer, the object being a merchandise, a service, a property, or a legal interest; a digital indication of a contractual term of the electronic transfer; a system-wide condition associated with a network of computing nodes; a system-wide condition associated with a statistical distribution of at least a portion of electronic transfers within the network of computing nodes; how the electronic transfer is to be carried out; whether the source account, the destination account, or the third account is anonymous; whether the transfer amount is backed by physical good or property; whether the transfer amount is backed by nationally issued currency; or any combination thereof.

[0034] The computing node can access, in step 508, an obligatory distribution rule object in its local cache to determine how the transfer amount is to be distributed amongst the destination account and at least a third account. Upon retrieving the obligatory distribution rule object, the computing node can authenticate the obligatory distribution rule object with at least a sponsor server in step 510. In various embodiments, the computer node can authenticate the obligatory distribution rule object with other external servers, including other computing notes of the electronic transfer system.

[0035] Once the conditional circumstance is determined and the obligatory distribution rule object is authenticated, the computing node generates, in step 512, a second digital string based at least partly on the obligatory distribution rule object, the conditional circumstance, and the first digital string to modify the electronic transfer to distribute a portion of the transfer amount to the third account. The computing node then publishes, in step 514, the second digital string electronically to other nodes in the electronic transfer system to represent a modified electronic transfer in accordance with the obligatory distribution rule object.

[0036] While processes or blocks are presented in a given order in **FIG. 5**, alternative embodiments may perform routines having steps, or employ systems having blocks, in a different order, and some processes or blocks may be deleted, moved, added, subdivided, combined, and/or modified to provide alternative or subcombinations. Each of these processes or blocks may be implemented in a variety of different ways. In addition, while processes or blocks are at times shown as being performed in series, these processes or blocks may instead be performed in parallel, or may be performed at different times.

[0037] **FIG. 6** is a block schematic diagram that depicts a machine in the exemplary form of a computer system 600, such as the computing node 400 of **FIG. 4**, within which a set of instructions for causing the machine to perform any of the herein disclosed methodologies may be executed. In alternative embodiments, the machine may comprise or

JPMC Ex. 1002
Page 654

include a network router, a network switch, a network bridge, personal digital assistant (PDA), a cellular telephone, a Web appliance or any machine capable of executing or transmitting a sequence of instructions that specify actions to be taken. The computer system 600 is intended to illustrate a hardware device on which any of the instructions, processes, modules and components depicted in the examples in **FIGs. 3-5** (and any other processes, techniques, modules, and/or components described in this specification) can be implemented. As shown, the computer system 600 includes a processor 602, memory 604, non-volatile memory 606, and a network interface 608. Various common components (*e.g.*, cache memory) are omitted for illustrative simplicity. The computer system 600 can be of any applicable known or convenient type, such as a personal computer (PC), or a server-class computer or mobile device (*e.g.*, smartphone, card reader, tablet computer, etc.). The components of the computer system 600 can be coupled together via a bus and/or through any other known or convenient form of interconnect.

[0038] One of ordinary skill in the relevant art will recognize that the terms "machine-readable (storage) medium" or "computer-readable (storage) medium" include any type of device that is accessible by the processor 602. The memory 604 is coupled to the processor 602 by, for example, a bus 610. The memory 604 can include, by way of example but not limitation, random access memory (RAM), such as dynamic RAM (DRAM) and static RAM (SRAM). The memory 604 can be local, remote, or distributed.

[0039] The bus 610 also couples the processor 602 to the non-volatile memory 606 and drive unit 612. The non-volatile memory 606 may be a hard disk, a magnetic-optical disk, an optical disk, a read-only memory (ROM), such as a CD-ROM, Erasable Programmable Read-Only Memory (EPROM), or Electrically Erasable Programmable Read-Only Memory (EEPROM), a magnetic or optical card, or another form of storage for large amounts of data. The non-volatile memory 606 can be local, remote, or distributed.

[0040] The data structures, modules, and instruction steps described in **FIGs. 3-5** may be stored in the non-volatile memory 606, the drive unit 612, or the memory 604. The processor 602 may execute one or more of the modules stored in the memory components.

[0041] The bus 610 also couples the processor 602 to the network interface 608. The network interface 608 can include one or more of a modem or network interface. A modem or network interface can be considered to be part of the computer system 600. The network interface 608 can include an analog modem, ISDN modem, cable modem, token ring interface, satellite transmission interface (*e.g.*, "direct PC"), or other interfaces for coupling a computer system to other computer systems.

JPMC Ex. 1002
Page 655

[0042] It is to be understood that embodiments may be used as, or to support, software programs or software modules executed upon some form of processing core (such as the CPU of a computer) or otherwise implemented or realized upon, or within, a machine or computer readable medium. A machine-readable medium includes any mechanism for storing or transmitting information in a form readable by a machine, *e.g.,* a computer. For example, a machine readable medium includes read-only memory (ROM); random access memory (RAM); magnetic disk storage media; optical storage media; flash memory devices; electrical, optical, acoustical or other form of propagated signals, such as, carrier waves, infrared signals, digital signals, etc.; or any other type of media suitable for storing or transmitting information.

[0043] Although system and methods are described herein with reference to one or more embodiments, one skilled in the art will readily appreciate that other applications may be substituted for those set forth herein without departing from the spirit and scope of the disclosure.

[0044] Some embodiments of the disclosure have other aspects, elements, features, and steps in addition to or in place of what is described above. These potential additions and replacements are described throughout the rest of the specification. For example, some embodiments include a method of operating a computing node in an electronic transfer system. The electronic transfer system can include a distributed computer system implemented by a network of delegation nodes for facilitating secure electronic transactions. The computing node can be one of the delegation nodes, or a computing device with network access to the delegation nodes. The method advantageously provides a mechanism to facilitate the anonymous or pseudo-anonymous electronic transfers in a distributed manner (e.g., without a centralized server system) while enforcing transfer-related rules managed by a central entity. This mechanism provides a technical solution to the technical problem (e.g., difficulty in transfer-related rule enforcement) faced in implementing the electronic transfer system, such as a distributed consensus system.

[0045] The method can include the computing node receiving a first digital string (e.g., an electronic record) representing an electronic transfer of a transfer amount from a source account to a destination account. The first digital string can be cryptographically signed with a private key corresponding to the source account and/or a private key corresponding to the destination account. Receiving the first digital string can include receiving the first digital string from another computer node with an indication to propagate and publish the first digital string to other nodes in the network. Receiving the first digital

JPMC Ex. 1002
Page 656

string can include receiving the first digital string via a local application executed by a processor. The local application can provide a user interface on a local display component for a user to certify that the user is an owner of the source account through a local input component.

[0046] The computing node can then verify availability of the transfer amount from the source account in a transaction history database. The transaction history database can maintain transaction records for all electronic transfers that ever occurred through the distributed consensus system (e.g., the electronic transfer system). The transaction history database may be available as a public ledger provided by the distributed consensus system .

[0047] For example, the distributed consensus system can include multiple delegation nodes (e.g., computing devices). The public ledger can be maintained in a distributed manner, such as a block chain, in these delegation nodes. The block chain keeps track of all confirmed electronic transfers that are reported to the distributed consensus system.

[0048] In several embodiments, the block chain confirms the electronic transfers via the distributed consensus system. The distributed consensus system confirms waiting electronic transfers by including them in the block chain. The distributed consensus system enforces a chronological order in the block chain and hence protects the neutrality of a network of delegation nodes that implements the public ledger. This enables the block chain to keep track of multiple electronic transfers in sequential groups (e.g., blocks). Any external computing device can access the block chain to verify that there is one or more cryptographically verified sequence of ancestor electronic transfers that sourced a given electronic transfer by accessing the block chain. If the given electronic transfer can be traced back to an origination of value (e.g., a cryptographically "minted" digital currency), then that given electronic transfer can be verified and confirmed.

[0049] In some embodiments, after verifying the availability of the transfer amount, the computing node determines a conditional circumstance of the electronic transfer. The computing node can access an obligatory distribution rule object. For example, the obligatory distribution rule object dictates how the transfer amount is distributed amongst the destination account and at least a third account. The computing node then authenticates the obligatory distribution rule object against a sponsor server (e.g., a computer server that has access to a public cryptographic key of a "sponsor". For example, the obligatory distribution rule object may be signed by a cryptographic signature using a private cryptographic key (e.g., corresponding to the public cryptographic key accessible to the sponsor server) of the sponsor. The sponsor server or another server with access to a corresponding public

JPMC Ex. 1002
Page 657

cryptographic key can verify the cryptographic signature of the obligatory distribution rule object .

[0050] For example, the conditional circumstance can include an attribute of the destination account, the source account, or the third account; an attribute of the electronic transfer; an identification of the source account, the destination account, or the third account; a location identifier of the source account, the destination account, or the third account; a time stamp of the electronic transfer; an account type (e.g., indicated as an enumeration for at least a non-profit organization account, a charity account, a religious entity account, a wholesaler account, a consumer account, a retailer account, a local business account, a service provider account, a large business account, a small business account, an international business account, or any combination thereof) of the source account, the destination account, or the third account; the transfer amount; a digital indication of an object (e.g., a merchandise, a service, a property, or a legal interest) of the electronic transfer; a digital indication of a contractual term of the electronic transfer; a system-wide condition associated with the network of the delegation nodes; a system-wide condition associated with a statistical distribution of at least a portion of electronic transfers within the network of the delegation nodes; how the electronic transfer is to be carried out (e.g., whether the electronic transfer is pre-authenticated or pre-validated, whether the source account, the destination account, or the third account is anonymous, whether the transfer amount is backed by at least a physical good or property, whether the transfer amount is backed by nationally issued currency, or any combination thereof), or any combination thereof.

[0051] In response to verifying the obligatory distribution rule object, the computing node can execute the distribution rule by generating a second digital string (e.g., an electronic record) based at least partly on the obligatory distribution rule object, the conditional circumstance, and the first digital string to modify the electronic transfer to distribute a portion of the transfer amount to the third account. For example, the computing node can generate the second digital string by matching the conditional circumstance to a rule entry of the obligatory distribution rule object and executing a distribution apportionment indication corresponding to the rule entry to modify the electronic transfer.

[0052] In some embodiments, the computing node can generate a transfer record corresponding to the second digital string and publish the transfer record to the public ledger. The computing node can publish the transfer record responsive to the obligatory distribution rule object being authenticated. For example, a delegation node of the distributed consensus system can incorporate the transfer record to a newly created block (e.g., containing a group

JPMC Ex. 1002
Page 658

of electronic transfers along with a proof-of-work indication) for appending to the end of the block chain. The delegation node can include the second digital string in the block responsive to the obligatory distribution rule object being authenticated. The computing node can then publish the block to the network of the delegation nodes in the distributed consensus system.

[0053] In some embodiments, the computing node can receive an indication from a user (e.g., verified user) of the source account. The indication can identify the third account based on the user's choice. In these embodiments, the portion of the transfer amount to the third account is dictated by the obligatory distribution rule object.

[0054] In some embodiments, the obligatory distribution rule object dictates at least a tax obligation within a sovereign governing entity, and the sponsor server is controlled by the sovereign governing entity. In some embodiments, the obligatory distribution rule object dictates a jurisdictional boundary of the sovereign governing entity and conditional circumstances that places an account beyond or within the jurisdictional boundary. For example, whether an electronic transfer falls within the jurisdictional boundary can be determined by a geographical location of the internet protocol (IP) address associated with the source account, the destination account, or the computing node.

[0055] In some embodiments, the obligatory distribution rule object dictates at least a fee owed to a credit issuer, and the sponsor server is controlled by the credit issuer. In some embodiments, the obligatory distribution rule object dictates at least a service fee owed to a service provider, and the sponsor server is controlled by the service provider. For example, the service provider can be a provider of digital currency; and the transfer amount is measured in that digital currency.

[0056] In some embodiments, the obligatory distribution rule object includes a conditional tree structure. Each node of the conditional tree structure can determine what conditions trigger a modification of the electronic transfer, how the transfer amount is to be distributed, who to distribute the amount to, or any combination thereof. For example, when the conditional circumstance of the computing node matches more than one node of the conditional tree structure, a branch node closer to the root node of the conditional tree structure governs how the transfer amount is to be distributed. In some embodiments, the obligatory distribution rule object includes a conditional tree structure. At least a branch node can correspond to a sub-sponsor that dictates a distribution apportionment of how the transfer amount is distributed but only if the distribution apportionment is consistent with conditional logics of a parent node of the branch node.

JPMC Ex. 1002
Page 659

[0057] For example, the obligatory distribution rule object includes a conditional tree structure with two or more levels. The root level can represent taxation required by a national sovereign government. A branch level can represent taxation required by local government or service fee requested by a service provider. For example, the obligatory distribution rule object can include a conditional tree structure with two or more levels. Authentication of the obligatory distribution rule object can include the computing node authenticating against a plurality of sponsor servers (e.g., including agents of the sponsor having the public key associated with the sponsor) corresponding to nodes in the obligatory distribution rule object. In this example, generating the second digital string can include determining which nodes of the obligatory distribution rule object apply to the electronic transfer. Here, the plurality of the sponsor servers can respectively correspond to the nodes that do apply to the electronic transfer in question.

[0058] In some embodiments, authenticating the obligatory distribution rule object includes receiving a cryptographic hash that solves a cryptographic puzzle. For example, the computing node can authenticate the obligatory distribution rule object by performing a mutual authentication using a challenge-response handshake in both directions between the computing node and the sponsor server.

[0059] In some embodiments, the obligatory distribution rule object dictates a jurisdictional boundary of a sponsor entity and conditional circumstances that places an account beyond or within the jurisdictional boundary. The sponsor entity can control the sponsor server. For example, the obligatory distribution rule object can dictate an increase of the transfer amount from the source account when the source account falls within the jurisdictional boundary. The obligatory distribution rule object can dictate a portion of the transfer amount that is to be deposited to the third account instead of the destination account when the destination account falls within the jurisdictional boundary. The account can indicate that it is within the jurisdictional boundary when the account has signed up for a service provided by the sponsor server or the sponsor entity. For example, the service provided by the sponsor entity or the sponsor server can include interest value generation, cache recovery, cryptographic key storage, risk management, accounting service, legal service, inflation protection, the reward or refund incentive, or any combination thereof. The service provided can also include providing allocation of at least a portion of digital currency implemented by the electronic transfer system that is lost due to shrinkage of the account.

[0060] In some embodiments, the computing node accesses the obligatory distribution rule object by retrieving the obligatory distribution rule object from a local cache on the

JPMC Ex. 1002
Page 660

computer node or retrieving it from a remote server. In some embodiments, the computing node can poll the sponsor server based on a schedule for updates to the obligatory distribution rule object. In some embodiments, the computing node can receive a push message from the sponsor server to update the obligatory distribution rule object. In some embodiments, the computing node can receive a push message from another node of the electronic transfer system to update the obligatory distribution rule object.

[0061] In some embodiments, when authentication of the obligatory distribution rule object fails, the computing node retrieves an updated instance of the obligatory distribution rule object from the sponsor server, verifies authenticity and/or data integrity of the updated instance, and caches the updated instance in the local cache of the computing node. In some embodiments, the computing node propagates the updated instance to at least another node in the network of the computer nodes.

[0062] The updated instance can include a certificate signature generated using a private cryptographic key known only to an operator of the sponsor server. The updated instance can include at least two certificate signatures generated with different private cryptographic keys. For example, authenticating the obligatory distribution rule object can include performing a bifurcated authentication with the at least two certificate signatures. In some embodiments, a previous instance of the obligatory distribution rule object can include a first certificate signature generated by a first private key that indicates that the previous instance is generated from the sponsor server and the updated instance of the obligatory distribution rule object can include a second certificate signature generated by a second private key corresponding to the first certificate signature that indicates that the previous instance is to be replaced by the updated instance.

[0063] While processes, steps, and functional components are described in a given order for the method, alternative embodiments may perform routines having steps, or employ systems having components, implemented in a different order, and some processes, steps or components may be deleted, moved, added, subdivided, combined, and/or modified to provide alternative or subcombinations. Each of these processes, steps, or components may be implemented in a variety of different ways. In addition, while processes, steps or components are at times described as being performed or executed in series, these processes, steps or components may instead be performed or executed in parallel, or may be performed or executed at different times.

[0064] The various steps in the method described above can be implemented in the computing node, such as the computer system 600 of **FIG. 1**. The processor 602 can execute

JPMC Ex. 1002
Page 661

any number of the steps or functions described above as configured by executable instructions stored in the memory 604 or the non-volatile memory 606.

JPMC Ex. 1002
Page 662

What is claimed is:

1. A method of operating a computing node in an electronic transfer system implemented by a network of computing nodes for facilitating secure electronic transactions, the method comprising:

receiving a first digital string representing an electronic transfer of a transfer amount from a source account to a destination account;

verifying availability of the transfer amount from the source account via a public ledger in a distributed consensus system;

determining a conditional circumstance of the electronic transfer;

accessing an obligatory distribution rule object, wherein the obligatory distribution rule object dictates how the transfer amount is distributed amongst the destination account and at least a third account;

authenticating the obligatory distribution rule object with a sponsor server; and

generating a second digital string based at least partly on the obligatory distribution rule object, the conditional circumstance, and the first digital string to modify the electronic transfer to distribute a portion of the transfer amount to the third account.

2. The method of claim 1, wherein generating the second digital string by matching the conditional circumstance to a rule entry of the obligatory distribution rule object and executing a distribution apportionment indication corresponding to the rule entry to modify the electronic transfer.

3. The method of claim 1, further comprising identifying the third account as indicated by a user of the source account; and wherein the portion of the transfer amount to the third account is dictated by the obligatory distribution rule object.

4. The method of claim 1, wherein the obligatory distribution rule object dictates at least a tax obligation within a sovereign governing entity, and wherein the sponsor server is controlled by the sovereign governing entity.

5. The method of claim 4, wherein the obligatory distribution rule object dictates a jurisdictional boundary of the sovereign governing entity and conditional circumstances that places an account beyond or within the jurisdictional boundary.

6. The method of claim 1, wherein the obligatory distribution rule object dictates at least a fee owed to a credit issuer, and wherein the sponsor server is controlled by the credit issuer.

JPMC Ex. 1002
Page 663

7. The method of claim 1, wherein the obligatory distribution rule object dictates at least a service fee owed to a service provider, and wherein the sponsor server is controlled by the service provider.

8. The method of claim 7, wherein the service provider is a provider of digital currency; and wherein the transfer amount is measured in that digital currency.

9. The method of claim 1, wherein the obligatory distribution rule object includes a conditional tree structure, wherein each node of the conditional tree structure determines what conditions trigger a modification of the electronic transfer, how the transfer amount is to be distributed, who to distribute the amount to, or any combination thereof.

10. The method of claim 9, wherein when the conditional circumstance of the computing node matches more than one node of the conditional tree structure, a branch node closer to a root node of the conditional tree structure governs how the transfer amount is to be distributed.

11. The method of claim 1, wherein the obligatory distribution rule object includes a conditional tree structure, wherein at least a branch node corresponds to a sub-sponsor that dictates a distribution apportionment of how the transfer amount is distributed but only if the distribution apportionment is consistent with conditional logics of a parent node of the branch node.

12. The method of claim 1, wherein the obligatory distribution rule object includes a conditional tree structure with two or more levels, wherein a root level represents taxation required by a national sovereign government, and a branch level represents taxation required by local government or service fee requested by a service provider.

13. The method of claim 1, wherein the obligatory distribution rule object includes a conditional tree structure with two or more levels, wherein authenticating the obligatory distribution rule object includes authenticating with a plurality of sponsor servers corresponding to nodes in the obligatory distribution rule object.

14. The method of claim 13, wherein generating the second digital string includes determining which nodes of the obligatory distribution rule object apply to the electronic transfer, and wherein the plurality of the sponsor servers respectively correspond to the nodes that apply to the electronic transfer.

15. The method of claim 1, wherein authenticating the obligatory distribution rule object includes receiving a cryptographic hash that solves a cryptographic puzzle.

JPMC Ex. 1002
Page 664

16. The method of claim 1, wherein authenticating the obligatory distribution rule object includes performing a mutual authentication by using a challenge-response handshake in both directions between the computing node and the sponsor server.

17. The method of claim 1, wherein the conditional circumstance includes an attribute of the destination account.

18. The method of claim 1, wherein the conditional circumstance includes an attribute of the source account.

19. The method of claim 1, wherein the conditional circumstance includes an attribute of the third account.

20. The method of claim 1, wherein the conditional circumstance includes an attribute of the electronic transfer.

21. The method of claim 1, wherein the conditional circumstance includes an identification of the source account, the destination account, or the third account.

22. The method of claim 1, wherein the conditional circumstance includes a location identifier of the source account, the destination account, or the third account.

23. The method of claim 1, wherein the conditional circumstance includes a time stamp of the electronic transfer.

24. The method of claim 1, wherein the conditional circumstance includes an account type of the source account, the destination account, or the third account.

25. The method of claim 24, wherein the account type is indicated as an enumeration for at least a non-profit organization account, a charity account, a religious entity account, a wholesaler account, a consumer account, a retailer account, a local business account, a service provider account, a large business account, a small business account, an international business account, or any combination thereof.

26. The method of claim 1, wherein the conditional circumstance includes the transfer amount.

27. The method of claim 1, wherein the conditional circumstance includes a digital indication of an object of the electronic transfer, the object being a merchandise, a service, a property, or a legal interest.

28. The method of claim 1, wherein the conditional circumstance includes a digital indication of a contractual term of the electronic transfer.

29. The method of claim 1, wherein the conditional circumstance includes a system-wide condition associated with a network of delegation nodes of the distributed consensus system.

JPMC Ex. 1002
Page 665

30. The method of claim 1, wherein the conditional circumstance includes a system-wide condition associated with a statistical distribution of at least a portion of electronic transfers within a network of delegation nodes of the distributed consensus system.

31. The method of claim 1, wherein the conditional circumstance includes how the electronic transfer is to be carried out.

32. The method of claim 31, wherein how the electronic transfer is to be carried out includes whether the electronic transfer is pre-authenticated or pre-validated.

33. The method of claim 31, wherein how the electronic transfer is to be carried out includes whether the source account, the destination account, or the third account is anonymous.

34. The method of claim 31, wherein how the electronic transfer is to be carried out includes whether the transfer amount is backed by at least a physical good or property.

35. The method of claim 31, wherein how the electronic transfer is to be carried out includes whether the transfer amount is backed by nationally issued currency.

36. A computing device, comprising:

a memory storing executable instructions;

a processor that is configured by the executable instructions to execute a process, the process comprising:

receiving a first electronic record representing an electronic transfer of a transfer amount from a source account to a destination account;

verifying availability of the transfer amount from the source account via a public ledger in a distributed consensus system;

determining a conditional circumstance of the electronic transfer;

accessing an obligatory distribution rule object, wherein the obligatory distribution rule object dictates how the transfer amount is distributed amongst the destination account and at least a third account;

authenticating the obligatory distribution rule object with a sponsor server; and

generating a second electronic record based at least partly on the obligatory distribution rule object, the conditional circumstance, and the first electronic record to modify the

JPMC Ex. 1002
Page 666

electronic transfer to distribute a portion of the transfer amount to the third account.

37. The computing device of claim 36, wherein receiving the first electronic record includes receiving the first electronic record from another computer node with an indication to propagate and publish the first electronic record to other nodes in network connection with the computing device.

38. The computing device of claim 36, wherein receiving the first electronic record includes receiving the first electronic record via a local application executed by a processor, the local application providing a user interface on a local display component for a user to certify that the user is an owner of the source account through a local input component.

39. The computing device of claim 36, wherein the process further comprises:

generating a transfer record corresponding to the second electronic record after the obligatory distribution rule object is authenticated; and

publishing the transfer record to be included in a block containing a group of recent electronic transfers, the block being appended to an end of a block chain representing the public ledger.

40. The computing device of claim 36, wherein the obligatory distribution rule object dictates a jurisdictional boundary of a sponsor entity and conditional circumstances that places an account beyond or within the jurisdictional boundary; and wherein the sponsor entity controls the sponsor server.

41. The computing device of claim 40, wherein the obligatory distribution rule object dictates an increase of the transfer amount from the source account when the source account falls within the jurisdictional boundary.

42. The computing device of claim 40, wherein the obligatory distribution rule object dictates a portion of the transfer amount that is to be deposited to the third account instead of the destination account when the destination account falls within the jurisdictional boundary.

43. The computing device of claim 40, wherein the account is within the jurisdictional boundary when the account has signed up for a service provided by the sponsor server or the sponsor entity.

44. The computing device of claim 43, wherein the service provided includes interest generation, cache recovery, cryptographic key storage, risk management, accounting

JPMC Ex. 1002
Page 667

service, legal service, inflation protection, reward or refund incentive, or any combination thereof.

45. The computing device of claim 43, wherein the service provided includes allocating at least a portion of digital currency implemented by an electronic transfer system that is lost due to shrinkage of the account.

46. The computing device of claim 36, wherein accessing the obligatory distribution rule object comprises retrieving the obligatory distribution rule object from a local cache on the computing device.

47. The computing device of claim 46, wherein the process further comprises polling the sponsor server based on a schedule for updates to the obligatory distribution rule object.

48. The computing device of claim 46, wherein the process further comprises receiving a push message from the sponsor server to update the obligatory distribution rule object.

49. The computing device of claim 46, wherein the process further comprises receiving a push message from another node of an electronic transfer system that the computing device is part of to update the obligatory distribution rule object.

50. The computing device of claim 46, wherein the process further comprises:

when authentication of the obligatory distribution rule object fails, retrieving an updated instance of the obligatory distribution rule object from the sponsor server;

verifying authenticity and data integrity of the updated instance; and

caching the updated instance in the local cache.

51. The computing device of claim 50, wherein the process further comprises propagating the updated instance to at least another node in a network of computer nodes that the computing device is part of; wherein the updated instance includes a certificate signature generated with a private cryptographic key known only to an operator of the sponsor server.

52. The computing device of claim 51, wherein the updated instance includes at least two certificate signatures generated with different private cryptographic keys.

53. The computing device of claim 52, wherein authenticating the obligatory distribution rule object includes performing a bifurcated authentication with the at least two certificate signatures.

54. The computing device of claim 50, wherein a previous instance of the obligatory distribution rule object includes a first certificate signature generated by a first

JPMC Ex. 1002
Page 668

private key that indicates that the previous instance is generated from the sponsor server; and wherein the updated instance of the obligatory distribution rule object includes a second certificate signature generated by a second private key corresponding to the first certificate signature that indicates that the previous instance is to be replaced by the updated instance.

5

JPMC Ex. 1002
Page 669

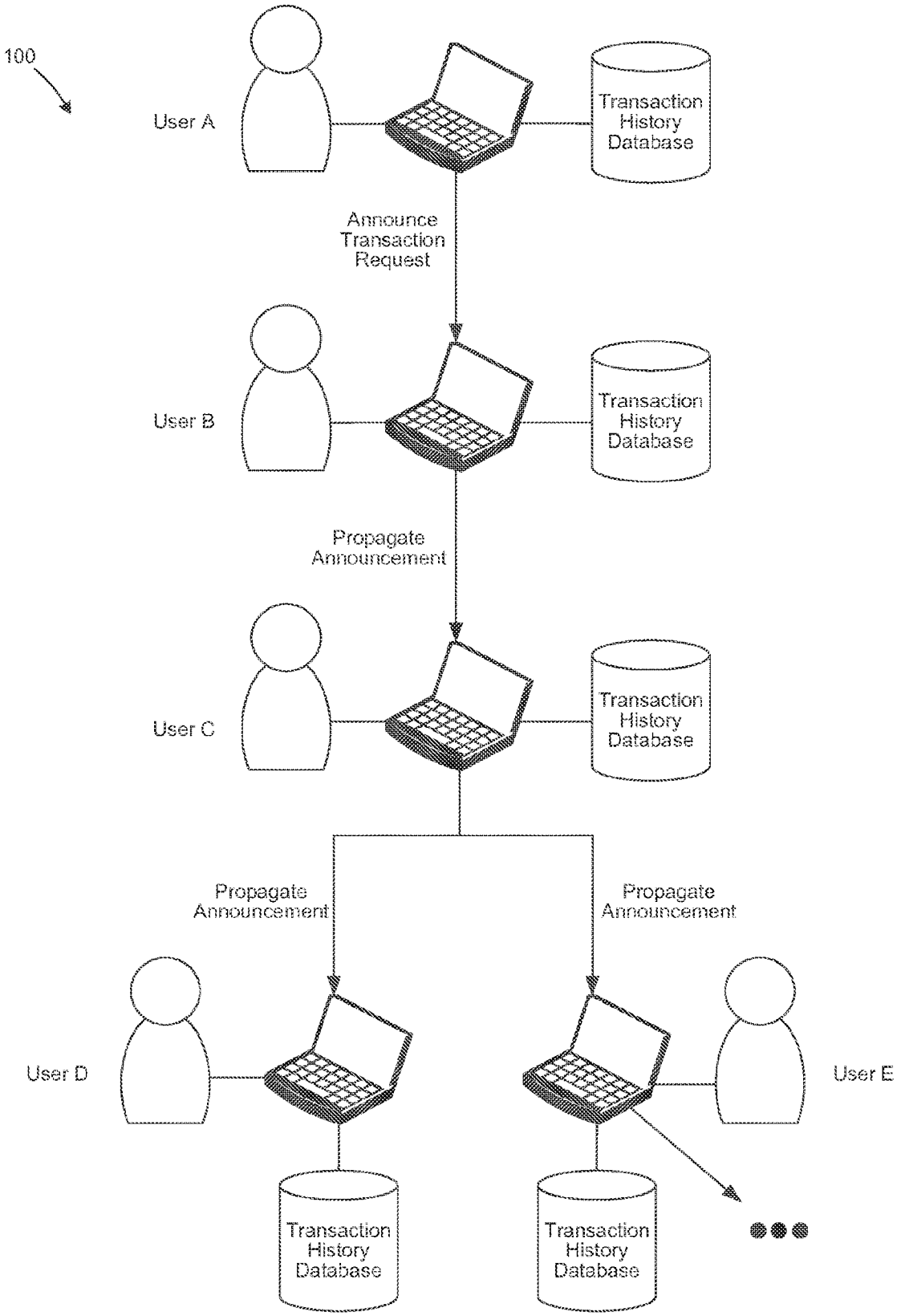


FIG. 1

JPMC Ex. 1002
Page 670

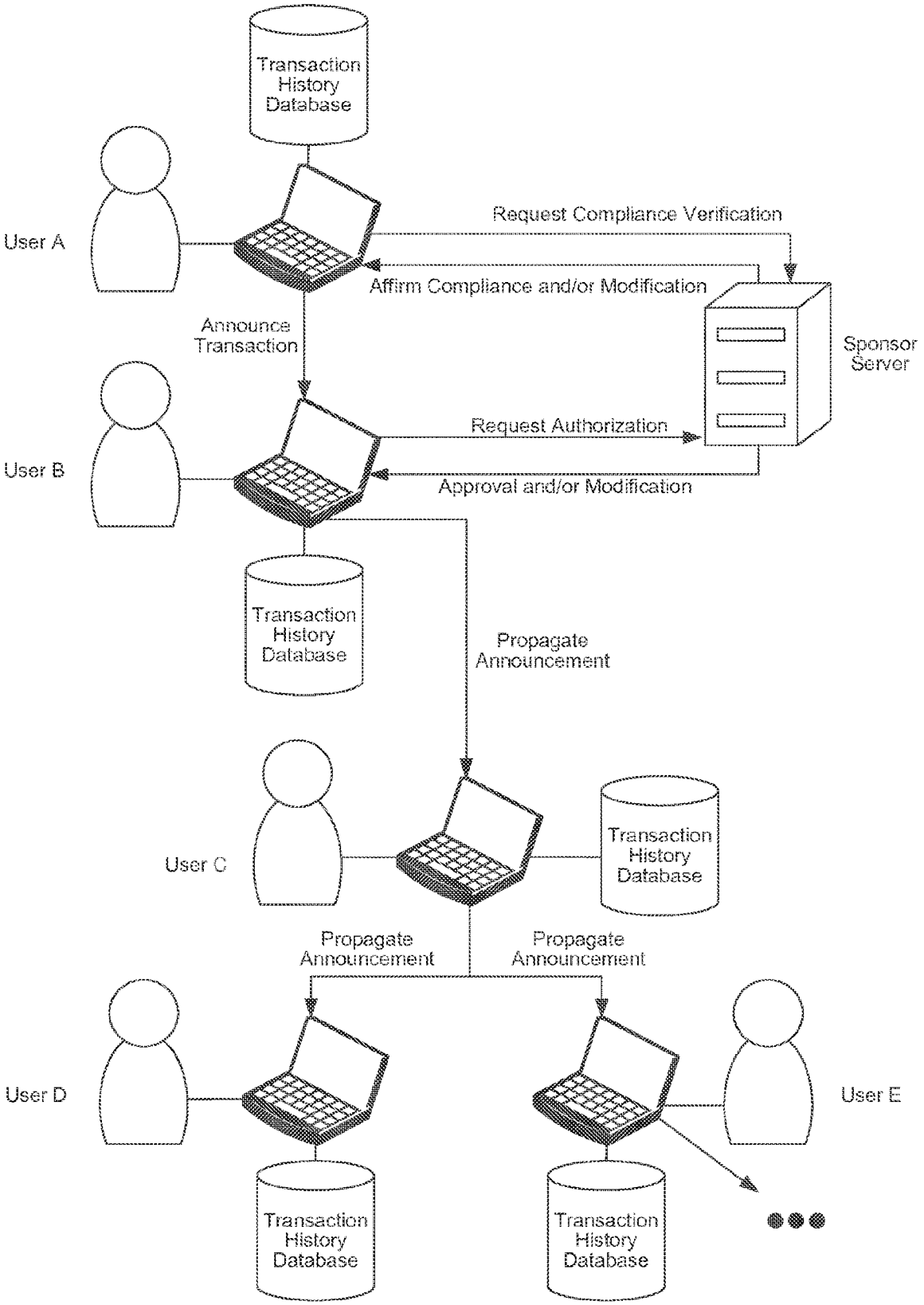


FIG. 2

JPMC Ex. 1002
Page 671

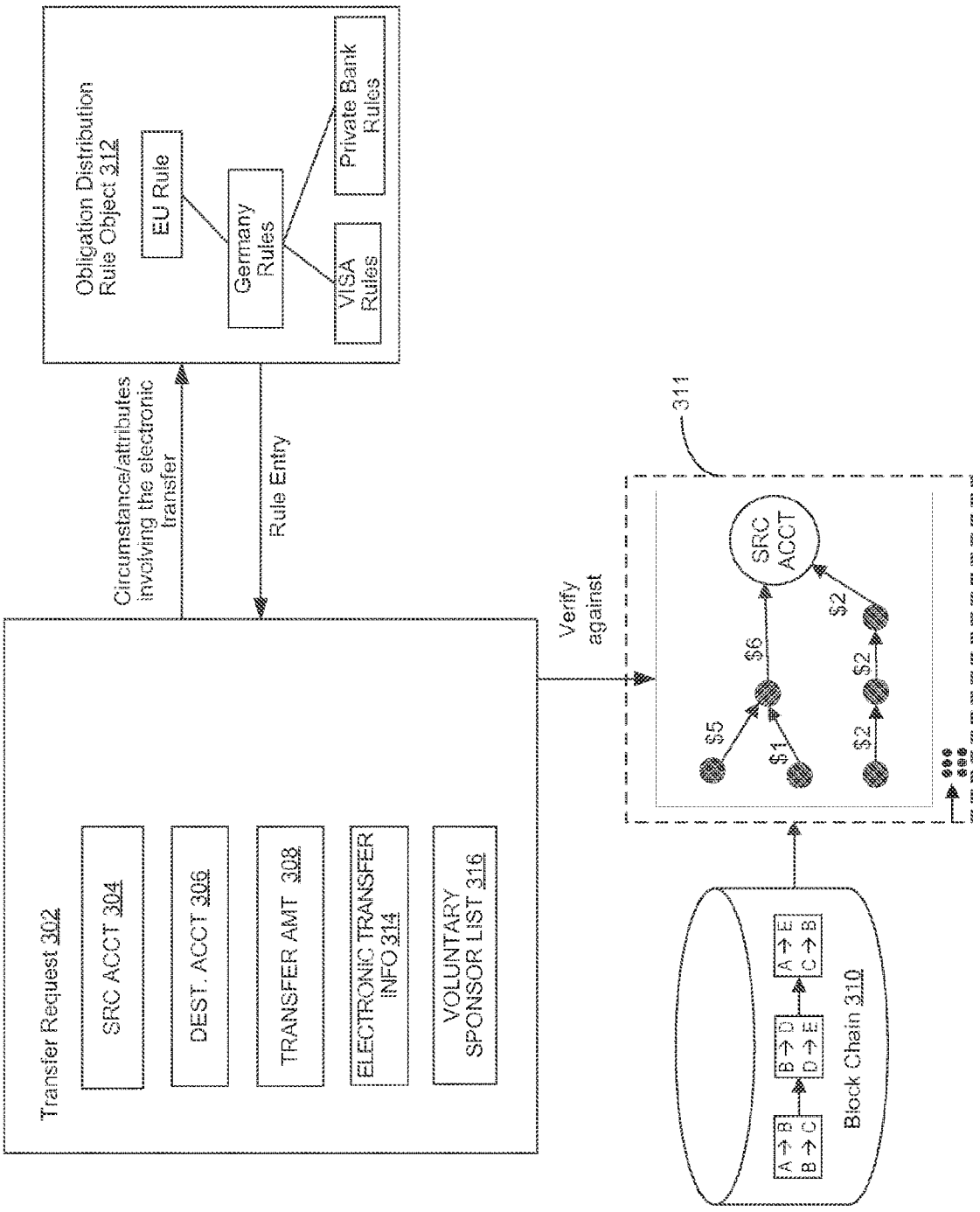


FIG. 3

JPMC Ex. 1002
Page 672

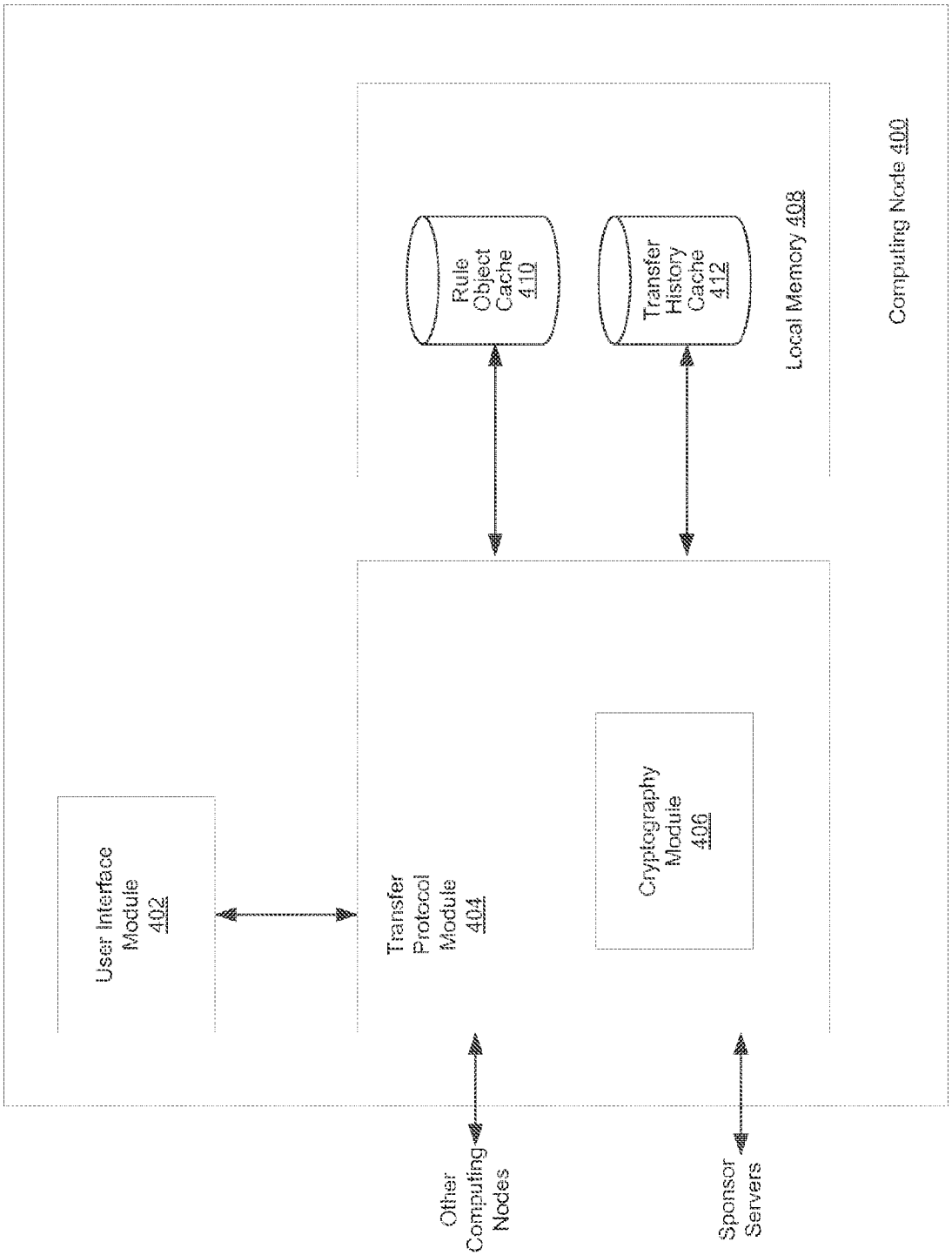


FIG. 4

JPMC Ex. 1002
Page 673

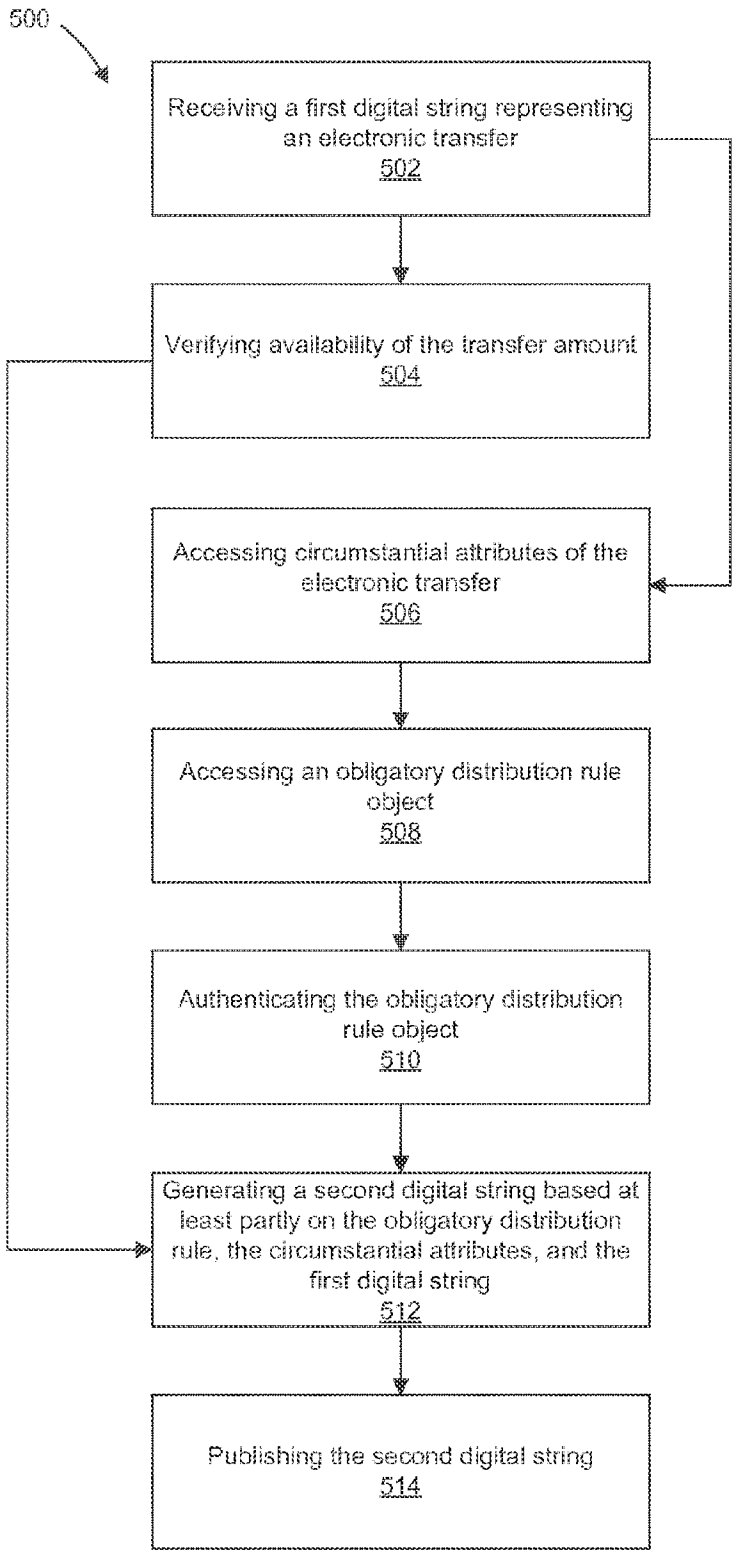


FIG. 5

JPMC Ex. 1002
Page 674

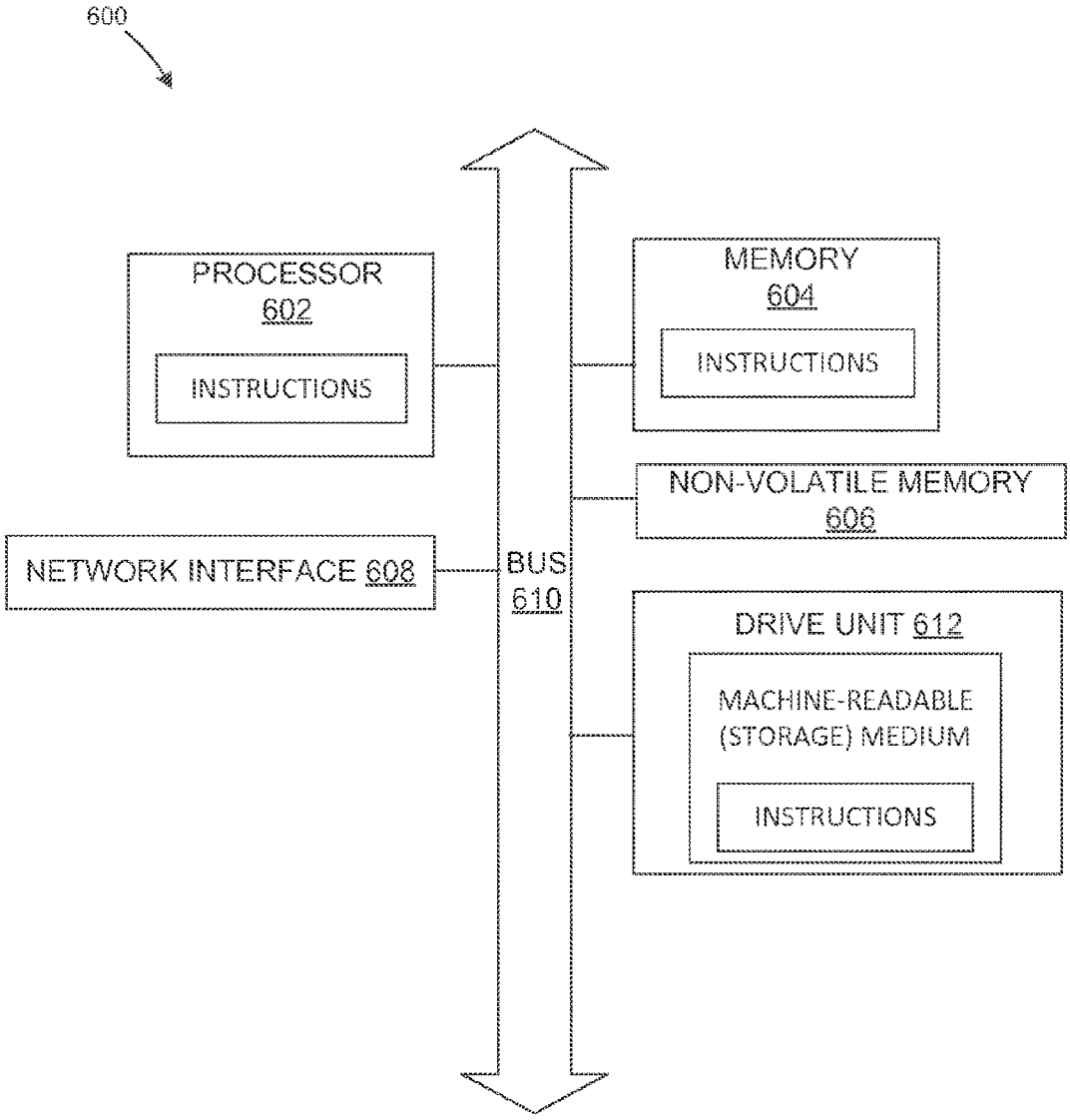


FIG. 6

JPMC Ex. 1002
Page 675

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2016/000279

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/38 (2012.01) G06F 17/30 (2006.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

wpiap, epodoc: ipc g06f, g06q, h04l, g07c & keywords (block chain, hash chain, hash tree, merkle tree, ledger, register, registrar distributed, electronic, ownership, document, title, certificate, contract, transaction, financial, enrich, combine, merge, append, join, chain, token, attribute, hash, checksum, stamp, timestamp, watermark) & like terms; txte: keywords (block chain, hash chain, hash tree, merkle tree, ledger, register, registrar, distributed, electronic, ownership, document, title, certificate, contract, enrich, combine, merge, append, join, chain, token, hash, timestamp) & like terms; google scholar: keywords (enrich, token, block chain, document, combine, merge, append join); espacenet: ipc g06 & keywords (block chain, document stamp token); ipa internal: inventor & applicant

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	Documents are listed in the continuation of Box C	

[X] Further documents are listed in the continuation of Box C [X] See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
1 November 2016	01 November 2016

Name and mailing address of the ISA/AU

AUSTRALIAN PATENT OFFICE
PO BOX 200, WODEN ACT 2606, AUSTRALIA
Email address: pct@ipaustralia.gov.au

Authorised officer

Peter Garay
AUSTRALIAN PATENT OFFICE
(ISO 9001 Quality Certified Service)
Telephone No. +61262832451

INTERNATIONAL SEARCH REPORT		International application No.
C (Continuation).	DOCUMENTS CONSIDERED TO BE RELEVANT	PCT/AU2016/000279

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2015/116998 A2 (KREMEN) 06 August 2015 The whole document, especially abstract, figs 2, 3, 5, §0013-0014, 0017, 0018, 0022, 0045, 0058, 0059	1-58
A	US 2009/0100041 A1 (WILSON) 16 April 2009 The whole document	
A	US 2011/0184910 A1 (LOVE et al.) 28 July 2011 The whole document	
A	EP 2843587 A1 (OPENLIMIT SIGNCUBES AG) 04 March 2015 The whole document	
A	US 2004/0006692 A1 (HONDA et al.) 08 January 2004 The whole document	
A	US 2008/0201580 A1 (SAVITZKY et al.) 21 August 2008 The whole document	
A L	Snow, P., et al. "Factom Ledger by Consensus." [retrieved from internet on 25 October 2016]. < URL: http://bravenewcoin.com/assets/Whitepapers/FactomLedgerbyConsensus.pdf > (The International Searching Authority is unable to establish the publication date of the above citation). The whole document	
A	Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008). [retrieved from internet on 25 October 2016]. < URL: http://web.archive.org/web/20150616021417/http://www.cryptovest.co.uk/resources/Bitcoin%20paper%20Original.pdf > published on or before 16 June 2015 as per Wayback Machine The whole document	

JPMC Ex. 1002
Page 677

INTERNATIONAL SEARCH REPORT Information on patent family members	International application No. **PCT/AU2016/000279**

This Annex lists known patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document/s Cited in Search Report		**Patent Family Member/s**	
Publication Number	**Publication Date**	**Publication Number**	**Publication Date**
WO 2015/116998 A2	06 August 2015	WO 2015116998 A2	06 Aug 2015
US 2009/0100041 A1	16 April 2009	US 2009100041 A1	16 Apr 2009
		US 7904450 B2	08 Mar 2011
		US 2011125718 A1	26 May 2011
		US 8135714 B2	13 Mar 2012
		US 2013282678 A1	24 Oct 2013
		US 8903839 B2	02 Dec 2014
		US 2012197901 A1	02 Aug 2012
		US 9053142 B2	09 Jun 2015
		US 2015254459 A1	10 Sep 2015
		US 9330261 B2	03 May 2016
		US 2016212146 A1	21 Jul 2016
US 2011/0184910 A1	28 July 2011	US 2011184910 A1	28 Jul 2011
		US 9122729 B2	01 Sep 2015
EP 2843587 A1	04 March 2015	EP 2843587 A1	04 Mar 2015
US 2004/0006692 A1	08 January 2004	US 2004006692 A1	08 Jan 2004
		US 7249258 B2	24 Jul 2007
		JP 2004040344 A	05 Feb 2004
US 2008/0201580 A1	21 August 2008	US 2008201580 A1	21 Aug 2008
		US 8006094 B2	23 Aug 2011
		EP 1962222 A2	27 Aug 2008
		JP 2008206158 A	04 Sep 2008
		US 2012017093 A1	19 Jan 2012
		US 8412946 B2	02 Apr 2013

End of Annex

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of

ARMSTRONG et al.

Application No.: To be Assigned

Filed: Concurrently Herewith

Atty Dkt. No.: AMK-5243-0009

Confirmation No.: To be Assigned

Art Unit: To be Assigned

Examiner: To be Assigned

Title: COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR

Date: February 14, 2018

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450
Sir:

INFORMATION DISCLOSURE STATEMENT

Pursuant to 37 C.F.R. 1.56, the attention of the Patent and Trademark Office is hereby directed to the reference(s) listed on the attached Form(s) PTO/SB/08 or equivalent. One copy of the reference(s) is attached. It is respectfully requested that the information be expressly considered during the prosecution of this application, and that the reference(s) be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

1. ☒ This Information Disclosure Statement ("IDS") is being filed within three (3) months of the U.S. filing date OR before the mailing date of a first Office Action on the merits. No certification or fee is required.
2. ☐ This IDS is being filed more than three (3) months after the U.S. filing date AND after the mailing date of the first Office Action on the merits, but before the mailing date of a Final Rejection or Notice of Allowance.
   - ☐ a. I hereby certify that each item of information contained in this IDS was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three (3) months ago to the filing of this IDS. 37 C.F.R. 1.97(e)(1);
   - ☐ b. I hereby certify that no item of information in this IDS was cited in any communication from a foreign patent office in a counterpart foreign application or, to my knowledge after making reasonable inquiry, was known to any individual designated in 37 CFR§1.56(c) more than three (3) months ago to the filing of this IDS. 37 C.F.R. 1.97(e)(2); OR
   - ☐ c. Payment in the amount of $240.00 (1806)/$120.00 (2806)/$60.00 (3806) of the fee under 37 C.F.R. 1.17(p) is submitted herewith. Please credit or debit Deposit Acct No. 14-1140 as needed to ensure consideration of the disclosed information.
3. ☐ This IDS is being filed more than three months after the U.S. filing date and after the mailing date of a Final Rejection or Notice of Allowance, but before payment of the Issue Fee. Payment in the amount of $240.00 (1806)/$120.00 (2806)/$60.00 (3806) of the fee under 37 C.F.R. 1.17(p) is submitted herewith. Please credit or debit Deposit Account No. 14-1140 as needed to ensure consideration of the disclosed information.
   - ☐ a. I hereby certify that each item of information contained in this IDS was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three (3) months ago to the filing of this IDS. 37 C.F.R. 1.97(e)(1).
   - ☐ b. I hereby certify that no item of information in this IDS was cited in any communication from a foreign patent office in a counterpart foreign application or, to my knowledge after making reasonable inquiry, was known to any individual designated in 37 CFR§1.56(c) more than three (3) months ago to the filing of this IDS. 37 C.F.R. 1.97(e)(2).
4. ☐ Relevance of the non-English language reference(s) is discussed in the present specification.
5. ☒ The reference(s) was/were cited in a counterpart foreign application. An English language version of the foreign search report is attached for the Examiner's information.
6. ☐ A concise explanation of the relevance of the non-English language reference(s) appears in the Appendix hereto.
7. ☐ The Examiner's attention is directed to co-pending U.S. Patent Application No. _____, filed _____, which is directed to related technical subject matter. The identification of this U.S. Patent Application is not to be construed as a waiver of secrecy as to that application now or upon issuance of the present application as a patent. The Examiner is respectfully requested to consider the cited application and the art cited therein during examination.
8. ☐ Copies of the references were cited by or submitted to the Office in parent Application No. _____ (filed _____), which is relied upon for an earlier filing date under 35 U.S.C. 120. Thus, Form PTO/SB/08 or equivalent is attached without copies of these references. 37 C.F.R. 1.98(d).
9. ☐ Each item of Information contained in the Information Disclosure Statement:
   a) Was first cited in any communication from a patent office in a counterpart foreign or international application or from the Office, and this communication was not received by an individual designated in § 1.56(c) more than thirty days prior to the filing of the Information Disclosure Statement; and/or

   b) Is a communication that was issued by a patent office in a counterpart foreign or international application or by the Office, and this communication was not received by any individual designated in § 1.56(c) more than thirty days prior to the filing of the Information Disclosure Statement 37 C.F.R. 1.704(d).
10. ☐ Other:

901 North Glebe Road, 11th Floor
Arlington, Virginia 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100
AMK:jls

NIXON & VANDERHYE P.C.
By Atty: Alan M. Kagen, Reg. No. 36,178

Signature: /Alan M. Kagen/

INFORMATION DISCLOSURE CITATION	ATTY. DOCKET NO.	APPLICATION NO.
	AMK-5243-0009	To Be Assigned
	INVENTOR(S)	
	ARMSTRONG et al.	
(Use several sheets if necessary)	FILING DATE	ART UNIT
	Concurrently Herewith	To be Assigned

U.S. PATENT DOCUMENTS

*EXAMINER INITIALS		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
		2004/0006692	1/2004	Honda et al.			
		2008/0201580	8/2008	Savitzky et al.			
		2009/0100041	4/2009	Wilson			
		2011/0184910	7/2011	Love et al.			
		2014/0279519	9/2014	Mattes et al.			

FOREIGN PATENT DOCUMENTS

*EXAMINER INITIALS		DOCUMENT	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION YES	TRANSLATION NO
		2 843 587	3/2015	Europe				
		WO 2015/116998	8/2015	PCT				

OTHER DOCUMENTS (including Author, Title, Date, Pertinent pages, etc.)

		International Search Report dated November 1, 2016 issued in PCT International Patent Application No. PCT/AU2016/000279, 3 pp.
		Nakamoto, Satoshi et al., "Bitcoin: A Peer-to-Peer Electronic Cash System." (2008). [Retrieved from Internet on 25 October 2016]. URL: http://web.archive.org/web/20150616021417/http://www.cryptovest.co.uk/resources/Bitcoin%20paper%200riginal.pdf, published on or before 16 June 2015 as per Wayback Machine, 9 pp.
		Snow, Paul et al., "Factom Ledger by Consensus," [Retrieved from Internet on 25 October 2016]. URL: http ://bravenewcoin.com/assets/Whitepapers/FactomLedgerbyConsensus.pdf, January 17, 2015, 28 pp.

Examiner Signature		Date Considered	

*Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR
First Named Inventor/Applicant Name:	Nick Armstrong
Filer:	Alan Mark Kagen/Janet Stoy
Attorney Docket Number:	AMK-5243-9

Filed as Small Entity

Filing Fees for U.S. National Stage under 35 USC 371

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
BASIC NATIONAL STAGE FEE	2631	1	150	150
NATL STAGE SEARCH FEE - REPORT PROVIDED	2642	1	260	260
NATL STAGE EXAM FEE - ALL OTHER CASES	2633	1	380	380
Pages:				
NATL STAGE APPL SZ FEE PER 50 PGS >100	2681	1	200	200
Claims:				
Miscellaneous-Filing:				
OATH/DECL > 30 MOS FROM 371 COMMENCEMENT	2617	1	70	70

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**1060**

Electronic Acknowledgement Receipt

EFS ID:	31790211
Application Number:	15752711
International Application Number:	PCT/AU2016/000279
Confirmation Number:	5327
Title of Invention:	COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR
First Named Inventor/Applicant Name:	Nick Armstrong
Customer Number:	23117
Filer:	Alan Mark Kagen/Janet Stoy
Filer Authorized By:	Alan Mark Kagen
Attorney Docket Number:	AMK-5243-9
Receipt Date:	14-FEB-2018
Filing Date:	
Time Stamp:	14:18:05
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$1060
RAM confirmation Number	021518INTEFSW14193100
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal of New Application	5243-9_cvr_national_phase_app.pdf	43844 16f6a327cbd889c6ca0f38027422f441c2999e25	no	3
Warnings:					
Information:					
2	Application Data Sheet	5243-9_app_data_sheet.pdf	1796535 ecae8ffe4fb3651ce5804331777ec23637262cbd	no	10
Warnings:					
Information:					
3		5243-9_application.pdf	11774184 00083db205e7b6f6c7d88d86bac2db0883ebc2f6	yes	115

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Abstract	1	1
	Specification	2	76
	Claims	77	92
	Drawings-only black and white line drawings	93	115

Warnings:					
Information:					
4		5243-9_prel_amd.pdf	44796 eeb729603ba01fe0c49d42dddb28d5f136f28350	yes	11

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**

	Preliminary Amendment		1		1
	Abstract		2		2
	Specification		3		3
	Claims		4		9
	Applicant Arguments/Remarks Made in an Amendment		10		10
	Abstract		11		11
Warnings:					
Information:					
5	Foreign Reference	EP2843587A1.pdf	1199296 ecd4824f95eb788931adaaebc48a2a3b642895b1	no	12
Warnings:					
Information:					
6	Foreign Reference	WO2015116998A2.pdf	4637818 97c8b58a919098472b1bab360cafe4d1cc76082f	no	31
Warnings:					
Information:					
7	Non Patent Literature	Nakamoto.pdf	186126 f0bfd9acab61f4fc245800c7b45c5b0bc707a4b6	no	9
Warnings:					
Information:					
8	Non Patent Literature	Snow.pdf	1619086 94a83d3b2561cb1669ce5e6613250348f3c99b66	no	28
Warnings:					
Information:					
9	Other Reference-Patent/App/Search documents	5243-9_Intl_Search_Report.pdf	334116 c6d750d1aa287e9f5807ab797018261e233e227f	no	3
Warnings:					
Information:					

10		5243-9_ids.pdf	33751 00c9bd39986f591d18e37d34b97fcf26da95d7f8	yes	2

Multipart Description/PDF files in .zip description		
Document Description	**Start**	**End**
Transmittal Letter	1	1
Information Disclosure Statement (IDS) Form (SB08)	2	2

Warnings:

Information:

11	Fee Worksheet (SB06)	fee-info.pdf	38504 6de5479f8d2857b77f5204bc105456cb7a1e206b	no	2

Warnings:

Information:

Total Files Size (in bytes):	21708056

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Australian Government

PCT/AU2016/000279

Patent Office
Canberra

I, VIVIENNE IGLESIAS, DELEGATE OF THE COMMISSIONER, hereby certify that annexed is a true copy of the Provisional specification in connection with Application No. 2015903292 for a patent by SPARRO (AUSTRALIA) PTY LTD as filed on 14 August 2015.

WITNESS my hand this
THIRTEENTH day of September 2016

VIVIENNE IGLESIAS
DELEGATE OF THE COMMISSIONER

COMMONWEALTH OF AUSTRALIA
AUSTRALIA
PATENT OFFICE

14 Aug 2015 2015903292

Payment Messaging System

TECHNICAL FIELD

[0001] The present invention relates to settlement systems and, more particularly although not exclusively, to a payment messaging system particularly, although not exclusively, suited to electronic transactions.

BACKGROUND

[0002] "Settlement" in the sense of settling amounts owing as between two parties, whether in a Fiat currency or in the newer forms of electronic currency (such as "Bitcoin") is a known concept which is central to the workings of most financial systems. In the case of electronic currency which requires settlement by exchange of data between institutions the current system is quite cumbersome and leads to many costs due in part to the necessity for often repeated data entry of significant amounts of data into systems run by the parties to any given transaction requiring settlement and also to the intermediaries that it almost every instance (barring a non-electronic cash transaction) form part of a chain of intermediaries that become involved in ultimately effecting settlement of any given transaction.

[0003] In particular implementations of settlement systems across the internet, a block chain structure may be utilised where a block chain is a distributed database that maintains a continuously growing list of data records that may be hardened against tampering and revision. The most widely known application of a block chain is the public ledger of transactions for cryptocurrencies, such as Bitcoin referenced above.

[0004] Many settlement systems are characterised by effectively one-way transmission of data in any given data exchange transaction (for example systems based on Swift messaging). If it is subsequently discovered that there are deficiencies in the data thus transmitted there can then ensue time consuming checking and querying operations before settlement can be effected.

[0005] It is an object of the present invention to address or at least ameliorate some of the above disadvantages.

Notes

[0006] The term "comprising" (and grammatical variations thereof) is used in this specification in the inclusive sense of "having" or "including", and not in the exclusive sense of "consisting only of".

2015903292 14 Aug 2015

[0007] The above discussion of the prior art in the Background of the invention, is not an admission that any information discussed therein is citable prior art or part of the common general knowledge of persons skilled in the art in any country.

SUMMARY OF INVENTION

Definitions:

[0008] **token:** in this specification a "token" is a data record containing data required to settle a transaction for which the token has been generated; and wherein the data is rendered, formatted or passed through an algorithm in a predetermined manner. The process of rendering, formatting or passing through an algorithm in a predetermined manner is termed "tokenisation". The tokenisation process may involve operations such as encryption and de-identification of data.

[0009] **Transaction:** in this specification "transaction" refers to a trade between two parties, for example at least a first transacting entity and a second transacting entity and wherein the trade is expressed in a financial form (for example in a Fiat currency or an electronic currency-to be distinguished, for example, from a barter transaction) which will ultimately require exchange of currency to settle the transaction. In some instances the currency will be the same on both sides of the transaction. In other cases a conversion from one currency to another may be required.

[00010] Accordingly, in one broad form of the invention, there is provided a system for settling a transaction electronically; said system comprising:

at least a first transacting entity;

at least a second transacting entity;

at least a first intermediary entity;

at least a second intermediary entity;

in the case where the first transacting entity enters into a transaction with the second transacting entity generating a tokenised message at the time of the transaction containing data needed to settle the transaction;

initiating settlement of the transaction by transmission of the tokenised message to the at least first transacting entity.

[00011] In a further broad form of the invention there is provided a tokenised message construction system; said system comprising:

a server in communication with a database and which facilitates communications between a plurality of parties to a transaction;

2015903292 14 Aug 2015

each party having a digitised device with which to communicate with other ones of the parties and with the server;

each party capable of generating a tokenised message via a bidirectional communication with the server.

[00012] Preferably the tokenised message is generated with reference to a token database located at a remote location.

[00013] Preferably the tokenised message includes at least a first data element, a second data element and a third data element.

[00014] Preferably the first data element comprises identification data for a payor, the second data element comprises identification data for a payee (biller) and the third data element comprises identification currency, denomination and value data.

[00015] Preferably a further tokenised message is generated by either an intermediary entity or the token database.

[00016] Preferably a tokenised message is generated by a bi-directional communication process.

[00017] Preferably the bi-directional communication process is between the token database and an intermediary entity.

[00018] Preferably a step in producing a tokenised message involves de-identifying data.

[00019] Preferably a step in producing a tokenised message involves adding a data element to the message.

[00020] Preferably a step in producing a tokenised message involves removing a data element from the message.

[00021] Preferably a step in producing a tokenised message involves applying an algorithm to the data elements in the message.

[00022] Preferably the token database sequences the tokenised messages.

[00023] Preferably the token database sequences the tokenised messages and transmits the tokenised messages as payment data records to a block chain settlement system.

[00024] Preferably the block chain settlement system employs the Ripple protocol.

BRIEF DESCRIPTION OF DRAWINGS

[00025] Embodiments of the present invention will now be described with reference to the accompanying drawings wherein:

2015903292 14 Aug 2015

[00026] Figure 1A is a block diagram of the entities and intermediaries involved in a prior art electronic settlement system;

[00027] Figure 1B is a data and funds flow according to a prior art settlement system;

[00028] Figure 2A is a data and funds flow diagram according to an indicative embodiment of the present invention;

[00029] Figure *2C* is a block diagram of the basic infrastructure and components suited for use with embodiments of the present invention and

[00030] Figure 3 A, B, C comprise block diagrams of the steps in a settlement transaction in accordance with a first preferred embodiment of the present invention

0031] Figure 4 is a block diagram of salient characteristics of a messaging system 10 of the prior art as compared with the salient messaging characteristics of the system 210 enabled by the code of a second embodiment.

0032] Figure 5 illustrates the options for data content to be included in tokens in accordance with embodiments of the invention as described above.

0033] Figure 6 provides a comparison of characteristics of embodiments of the present invention as compared with the prior art Swift-based messaging system.

[00034]

DESCRIPTION OF EMBODIMENTS

[00035] With reference to Figure 1 there is illustrated in block form the basic components of a prior art settlement system. In many transactions there will be an at least first transacting entity 11 which enters into a transaction with an at least second transacting entity 12. The transaction may be as simple as the agreement by the first transacting entity 11 to sell a particular item or service to the second transacting entity 12. Typically the transaction will require settlement for an agreed amount expressed in a Fiat or other currency. In the vast majority of cases the at least first transacting entity 11 will be associated with an at least first intermediary entity 13, in this instance in the form of a bank A and similarly the second transacting entity 12 will be associated with an at least second

2015903292 14 Aug 2015

intermediary entity 14 in this instance in the form of bank B. The first transacting entity 11 will have a first bank account 15 at the first intermediary entity 13 whilst second transacting entity 12 will have a second bank account 16 at second intermediary entity 14. Settlement of any given transaction requires instruction given by first transacting entity 11 to its first intermediary entity 13 to pay an agreed amount from the first bank account 15 to the bank account comprising second bank account 16 of second intermediary entity 14 of second transacting entity 12. For these instructions to be carried out metadata in the form of payment metadata 17 must be assembled at the first intermediary entity 13 sufficient and exhaustive to communicate to the second intermediary entity 14 such that the agreed settlement amount is transmitted from bank A to bank B and more particularly to the specific accounts of the respective first transacting entity 11 and second transacting entity 12.

[00036] A similar transaction may be applied in reverse where the second transacting entity sells a good or service to first transacting entity 11. In such an instance the respective intermediaries, once having received the respective payment metadata 17 and exchanged that metadata 17 may elect to simply pay the difference 18 electronically as between the intermediaries to effect the multiple transactions. In some instances, particularly where the transaction is cross-border-for example the first intermediary entity 13 is in a first country whilst the second intermediary entity 14 is in a second country the metadata 17 may include what is known as a Swift code which is a substantially unique identifier for each intermediary entity involved in the transaction. However, for any given transaction, far more data than merely a unique identifier for each intermediary entity involved in a transaction is required in order for the appropriate settlement amounts to ultimately be recorded in the correct accounts and settle the transaction for the agreed amounts.

[00037] Figure 1B is a data and funds flow diagram of data and funds flow according to a prior art settlement system at the granular level. In this instance, with reference to figure 1B pay like components are numbered as for figure 1 a given transaction requiring settlement can be embodied as a bill 90 which will include payment data 91 and may include bank facilitation payment data 92 comprising, in this instance, a biller code and a transaction code. Banks which are party to this bank facilitation payment system permit data entry by entity B (or payer B) 12 into a database of bank B 14 by means of a bank application or web interface 14 B. Bank B may then add additional data to form metadata 17 which is sent to a third-party server 93 which utilises metadata 17 to trigger pay (settlement) of bill 90 from payer B bank 14 to biller A bank 13.

2015903292 14 Aug 2015

[00038] **Generalised Embodiment:**

With reference to Figure 2C there is illustrated a block diagram of the basic infrastructure and components suited for use with embodiments of the present invention. In this instance like components are numbered as for figure 1 except in the 100 series. So, for example, first transacting entity 11 becomes first transacting entity 111 in this embodiment with reference to figure 2C.

In this instance a settlement system 110 according to a generalised embodiment includes at least first transacting entity 111 which enters into a transaction with at least a second transacting entity 112. As previously these entities are associated with a respective first intermediary entity 113 and a second intermediary entity 114 in the form of bank A and bank B. Each of the first transacting entity 111 and a second transacting entity 112 has a respective account 115, 116 at their respective intermediary entities as illustrated in figure 2C

In this instance, in the event that first transacting entity 111 enters into a transaction with second transacting entity 112 then, at the time of entry into the transaction 120, a token 121 is generated. In this instance the token 121 is generated by at least first digital device 122 communicating with a token database 123. The token database 123 generates a token comprising a data file 124 containing all data that will ultimately be required to settle the transaction 120 including any necessary identifying information for the transacting entity is, their accounts and the intermediary entities. Settlement is effected by communication of the token 121 to bank A and then to bank B together with the appropriate flow of funds.

With reference to figure 2A at the granular level a bill 190 from a bill of 111 directed to a payer 112 contains bill data 191 and also token data of a token 121 residing within a code symbol 194 (in this instance a QR code). The token data includes pointer data pointing to data 195 on token database 123. The Dato 195 combined with bank ID data 114 permits the creation by token database 123 of a full payment record 196 which can be utilised to cause settlement of the bill 190 as against payer 112 via, in this instance, their respective banks 114, 113.

With reference to figure 2B the payment data record 196 is utilised has fed into a settlement network such as, for example a network 197 operating under the Ripple protocol thereby permitting substantially real-time settlement across multiple institutions and banks.

14 Aug 2015 2015903292

[00039] **First Embodiment:**

[00040] With reference to Figures 3 there is illustrated in block diagram form a first preferred embodiment of the present invention by way of a non-limiting example of a transaction. In this embodiment like components are numbered as for the previous embodiments except in the 200 series. So, for example, token 121 becomes token 221.

[00041] With reference to figure 3A the transaction system 210 is activated, as for the previous embodiment, when a transaction 220 is entered into between at least first transacting entity 211 and at least a second transacting entity 212 each dealing, for the purposes of this transaction, through respective intermediary entities 213, 214.

[00042] At the time of and as part of entry into the transaction 220 the first transacting entity 211 accesses token database 223 via digital device 222 executing via a web browser interface or via execution of an application running on a portable digital devices such as a mobile telephone or in a further alternative as a point-of-sale terminal in order to arrange for the database 223 to generate a token 221. In this instance the token 221 will include better data 224 including the recipient named, BIC, IBAN, destination country, mobile number, currency, business type, communication, payment amount. In this instance the token 221 including the metadata 224 is stored in the token database 223. In addition the first transacting entity 211 communicates the token 221 to a digital device 230 associated with second transacting entity 212. In this instance the communication is by way of initial transmission of the token 221 to digital device 222 which then on transmits the token via Internet 231 to digital device 230.

[00043] With reference to figure 3B, when ready to settle the transaction 220 the second transacting entity 212 "logs in" to a portal associated with second intermediary entity 214 and communicates the token 221. In this instance have the login can be executed via a web browser associated with digital device 230 which communicates via Internet 231 the token 221 to a digital processing system 232 (including at least a processor and a memory) associated with second intermediary entity 214. Substantially at the same time as part of seeking to settle the transaction 220:

[00044] Notification: token database 223 notifies second intermediary entity 214 to contact the token database 223 from which it receives a further token 221A.

[00045] Verification: token database 223 communicates with the processing system 232 of second intermediary entity 214 to verify that sufficient funds are located in account 216 as indicated in the meta data 224 to settle the transaction

[00046] Committing payer funds: payers bank debits payers account: payers bank sends notice to payer bank gateway: payers bank gateway calls token database 223 to get approved token:

2015903292 14 Aug 2015

[00047] Settlement: gateway of payers bank sends XRP to billers bank gateway: payers bank gateway notifies token database 223 of receipt:

[00048] Clearing: payer's bank Nostro account is debited subject to bank institution rules.

[00049] Embodiments of the invention can be implemented utilising the "Ripple" the framework, protocol and gateway-or more generally any block chain based framework. In a particular form the final settlement process can be enabled through a Ripple frame work thereby to facilitate substantially real-time settlement across multiple institutions and multiple banks.

[00050]

[00051] **Second Embodiment:**

Examples of tokenised messages and their generation and transmission are illustrated in pseudocode below. Reference to "sparro" is a reference to an instance of a token database123.

[00052] The previous, meta-data mode is first. It switches to minimal half way through

--

Bank:HSBC >> createUserCode >> Sparro:Sparro

{"id":"User:ABC Paper","name":"ABC Paper"}

(Creating Sparro User Code - Meta-data given can be used by other banks for compliance and for confirming payee with customers.)

--

Bank:MayBank >> createUserCode >> Sparro:Sparro

{"id":"User:XYZ Printing","name":"XYZ Printing"}

(Creating Sparro User Code - Meta-data given can be used by other banks for compliance and for confirming payee with customers.)

--

Sparro:Sparro >> createUserCode-reply >> Bank:HSBC

{"id":"User:ABC Paper","name":"ABC Paper","code":"65q3gdd"}

--

Sparro:Sparro >> createUserCode-reply >> Bank:MayBank

{"id":"User:XYZ Printing","name":"XYZ Printing","code":"70wqgx6"}

2015903292 14 Aug 2015

--

User:ABC Paper >> createInvoice >> Bank:HSBC

{"amount":{"amount":1000,"currency":"gbp"}}

--

Bank:HSBC >> createInvoiceCode >> Sparro:Sparro

{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd"}

(Creating Invoice Code - An invoice code is created by Sparro and connected to the bank.)

-

Sparro:Sparro >> createInvoiceCode-reply >> Bank:HSBC

{"code":"6tq6wcbad"}

--

Bank:HSBC >> createInvoice-reply >> User:ABC Paper

{"invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

Abc invoice { amount: { amount: 1000, currency: 'gbp' },
payee: '65q3gdd',
code: '6tq6wcbad' }

--

User:ABC Paper >> invoice >> User:XYZ Printing

{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}

-

User:XYZ Printing >> payInvoice >> Bank:MayBank

{"invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300}}

--

Bank:MayBank >> sendMoney >> BankGateway:MayBank

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300}}

--

BankGateway:MayBank >> getInvoice >> Sparro:Sparro

"6tq6wcbad"

(Sending Payment to Invoice - The payment is sent to the bank that created the invoice.)

2015903292 14 Aug 2015

--

Sparro:Sparro >> getInvoice-reply >> BankGateway:MayBank

{"bank":"Bank:HSBC","invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

--

BankGateway:MayBank >> transfer >> BankGateway:HSBC

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":"ripple-1"}

--

BankGateway:HSBC >> incomingTransfer >> Bank:HSBC

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":"ripple-1"}

--

BankGateway:HSBC >> transfer-reply >> BankGateway:MayBank

{"success":true,"owed":{"GBP":300}}

--

Bank:HSBC >> getInvoice >> Sparro:Sparro

"6tq6wcbad"

--

BankGateway:MayBank >> sendMoney-reply >> Bank:MayBank

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":"ripple-1"}

--

Sparro:Sparro >> getInvoice-reply >> Bank:HSBC

{"bank":"Bank:HSBC","invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

2015903292 14 Aug 2015

--

Bank:MayBank >> payInvoice-reply >> User:XYZ Printing

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":
"ripple-1"}

XYZ part-paid invoice {
 "payer": "70wqgx6",
 "invoice": "6tq6wcbad",
 "amount": {
  "currency": "GBP",
  "amount": 300
 },
 "id": "ripple-1"
}

--

Bank:HSBC >> incomingTransfer >> User:ABC Paper

{"invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcb
ad"},"transfer":{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amo
unt":300},"id":"ripple-1"}}

-

User:XYZ Printing >> payInvoice >> Bank:MayBank
 {"invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700}}

--

Bank:MayBank >> sendMoney >> BankGateway:MayBank
 {"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700}}

--

BankGateway:MayBank >> getInvoice >> Sparro:Sparro
 "6tq6wcbad"

14 Aug 2015 2015903292

(Sending Payment to Invoice - The payment is sent to the bank that created the invoice.)

--

Sparro:Sparro >> getInvoice-reply >> BankGateway:MayBank

{"bank":"Bank:HSBC","invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

--

BankGateway:MayBank >> transfer >> BankGateway:HSBC

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700},"id":"ripple-2"}

--

BankGateway:HSBC >> incomingTransfer >> Bank:HSBC

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700},"id":"ripple-2"}

--

BankGateway:HSBC >> transfer-reply >> BankGateway:MayBank

{"success":true,"owed":{"GBP":1000}}

--

Bank:HSBC >> getInvoice >> Sparro:Sparro

"6tq6wcbad"

-

BankGateway:MayBank >> sendMoney-reply >> Bank:MayBank

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700},"id":"ripple-2"}

2015903292 14 Aug 2015

--

Sparro:Sparro >> getInvoice-reply >> Bank:HSBC

{"bank":"Bank:HSBC","invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

--

Bank:MayBank >> payInvoice-reply >> User:XYZ Printing

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700},"id":"ripple-2"}

XYZ finished paying invoice {
 "payer": "70wqgx6",
 "invoice": "6tq6wcbad",
 "amount": {
  "currency": "GBP",
  "amount": 700
 },
 "id": "ripple-2"
}

--- SWITCHING TO MODE: minimal ---

--

Bank:HSBC >> incomingTransfer >> User:ABC Paper

{"invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"},"transfer":{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700},"id":"ripple-2"}}

--Bank:HSBC >> createUserCode >> Sparro:Sparro

2015903292 14 Aug 2015

undefined
(Creating Sparro User Code - No meta-data is required.)

--
Bank:MayBank >> createUserCode >> Sparro:Sparro
undefined
(Creating Sparro User Code - No meta-data is required.)

--
Sparro:Sparro >> createUserCode-reply >> Bank:HSBC
{"code":"dnt7gec"}

--
Sparro:Sparro >> createUserCode-reply >> Bank:MayBank
{"code":"6wwpwuc"}

--
User:ABC Paper >> createInvoice >> Bank:HSBC
{"amount":{"amount":2000,"currency":"gbp"}}

--
Bank:HSBC >> createInvoiceCode >> Sparro:Sparro
null
(Creating Invoice Code - An invoice code is created by Sparro and connected to the bank. No invoice details are required.)

--
Sparro:Sparro >> createInvoiceCode-reply >> Bank:HSBC
{"code":"erwkax1md"}

--Bank:HSBC >> createInvoice-reply >> User:ABC Paper

2015903292 14 Aug 2015

{"invoice":{"amount":{"amount":2000,"currency":"gbp"},"code":"erwkax1md","payee":"User:
ABC Paper","transfers":[]}}

Abc invoice { amount: { amount: 2000, currency: 'gbp' },
code: 'erwkax1md',
payee: 'User:ABC Paper',
transfers: [] }

--

User:ABC Paper >> invoice >> User:XYZ Printing

{"amount":{"amount":2000,"currency":"gbp"},"code":"erwkax1md","payee":"User:ABC
Paper","transfers":[]}

--

User:XYZ Printing >> payInvoice >> Bank:MayBank

{"invoice":"erwkax1md","amount":{"currency":"GBP","amount":600}}

--

Bank:MayBank >> sendMoney >> BankGateway:MayBank

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600}}

--

BankGateway:MayBank >> getInvoice >> Sparro:Sparro

"erwkax1md"

(Sending Payment to Invoice - The payment is sent to the bank that created the invoice.)

--

Sparro:Sparro >> getInvoice-reply >> BankGateway:MayBank

{"bank":"Bank:HSBC"}

--

BankGateway:MayBank >> transfer >> BankGateway:HSBC

2015903292 14 Aug 2015

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}

--

BankGateway:HSBC >> incomingTransfer >> Bank:HSBC

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}

--

BankGateway:HSBC >> transfer-reply >> BankGateway:MayBank

{"success":true,"owed":{"GBP":600}}

--

Bank:HSBC >> incomingTransfer >> User:ABC Paper

{"invoice":{"amount":{"amount":2000,"currency":"gbp"},"code":"erwkax1md","payee":"User:ABC Paper","transfers":[{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}]},"transfer":{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}}

--

BankGateway:MayBank >> sendMoney-reply >> Bank:MayBank

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}

--

Bank:MayBank >> payInvoice-reply >> User:XYZ Printing

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}

14 Aug 2015 2015903292

XYZ part-paid invoice {
"payer": "6wwpwuc",
"invoice": "erwkax1md",
"amount": {
"currency": "GBP",
"amount": 600
},
"id": "ripple-3"
}
--
User:XYZ Printing >> payInvoice >> Bank:MayBank
{"invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400}}

--
Bank:MayBank >> sendMoney >> BankGateway:MayBank

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400}}

--
BankGateway:MayBank >> getInvoice >> Sparro:Sparro
"erwkax1md"
(Sending Payment to Invoice - The payment is sent to the bank that created the invoice.)

--
Sparro:Sparro >> getInvoice-reply >> BankGateway:MayBank
{"bank":"Bank:HSBC"}

-
BankGateway:MayBank >> transfer >> BankGateway:HSBC

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}

2015903292 14 Aug 2015

--

BankGateway:HSBC >> incomingTransfer >> Bank:HSBC

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}

BankGateway:HSBC >> transfer-reply >> BankGateway:MayBank

{"success":true,"owed":{"GBP":2000}}

--

Bank:HSBC >> incomingTransfer >> User:ABC Paper

{"invoice":{"amount":{"amount":2000,"currency":"gbp"},"code":"erwkax1md","payee":"User:ABC Paper","transfers":[{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"},{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}]},"transfer":{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}}

--

BankGateway:MayBank >> sendMoney-reply >> Bank:MayBank

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}

--

Bank:MayBank >> payInvoice-reply >> User:XYZ Printing

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}

2015903292 14 Aug 2015

```
XYZ finished paying invoice {
 "payer": "6wwpwuc",
 "invoice": "erwkax1md",
 "amount": {
  "currency": "GBP",
  "amount": 1400
 },
 "id": "ripple-4"
}
```

features of this embodiment include the enablement of a private, invitation only, network for banking institutions which, in a particular form, can facilitate cross-border payments thereby to enable substantially real-time payments at reduced processing cost.

With reference to figure 4 there is shown a block diagram of salient characteristics of a messaging system 10 of the prior art as compared with the salient messaging characteristics of the system 210 enabled by the code listed above and more broadly described with reference to the earlier embodiments.

figure 5 illustrates the options for data content to be included in tokens in accordance with embodiments of the invention as described above.

Figure 6 provides a comparison of characteristics of embodiments of the present invention as compared with the prior art Swift-based messaging system at a commercial layer 470, a security layer 471 and a technical layer 472.

[00053] The above describes only some embodiments of the present invention and modifications, obvious to those skilled in the art, can be made thereto without departing from the scope of the present invention.

2015903292 14 Aug 2015

CLAIMS

1. A system for settling a transaction electronically; said system comprising:
at least a first transacting entity;
at least a second transacting entity;

at least a first intermediary entity;
at least a second intermediary entity;
in the case where the first transacting entity enters into a transaction with the second transacting entity generating a tokenised message at the time of the transaction containing data needed to settle the transaction;
initiating settlement of the transaction by transmission of the tokenised message to the at least first transacting entity.

2. The system of claim 1 wherein the tokenised message is generated with reference to a token database located at a remote location.

3. The system of claim 2 wherein the tokenised message includes at least a first data element, a second data element and a third data element.

4. The system of claim 3 wherein the first data element comprises identification data for a payor, the second data element comprises identification data for a payee (biller) and the third data element comprises identification currency, denomination and value data.

5. The system of claim 1 or claim 2 wherein a further tokenised message is generated by either an intermediary entity or the token database.

6. The system of any previous claim where in a tokenised message is generated by a bi-directional communication process.

7. The system of claim 6 wherein the bi-directional communication process is between the token database and an intermediary entity.

8. The system of any previous claim wherein a step in producing a tokenised message involves de-identifying data.

9. The system of any previous claim wherein a step in producing a tokenised message involves adding a data element to the message.

10. The system of any previous claim wherein a step in producing a tokenised message involves removing a data element from the message.

11. The system of any previous claim wherein a step in producing a tokenised message involves applying an algorithm to the data elements in the message.

2015903292 14 Aug 2015

12. The system of any previous claim wherein the token database sequences the tokenised messages.

13. The system of any previous claim wherein the token database sequences the tokenised messages and transmits the tokenised messages as payment data records to a block chain settlement system.

14. The system of claim 13 wherein the block chain settlement system employs the Ripple protocol.

15. A tokenised message construction system; said system comprising:
a server in communication with a database and which facilitates communications between a plurality of parties to a transaction;
each party having a digitised device with which to communicate with other ones of the parties and with the server;
each party capable of generating a tokenised message via a bidirectional communication with the server.

16. The system of claim 15 wherein the tokenised message is generated with reference to a token database located at a remote location.

17. The system of claim 16 wherein the tokenised message includes at least a first data element, a second data element and a third data element.

18. The system of claim 17 wherein the first data element comprises identification data for a payor, the second data element comprises identification data for a payee (biller) and the third data element comprises identification currency, denomination and value data.

19. The system of claim 15 or claim 16 wherein a further tokenised message is generated by either an intermediary entity or the token database.

20. The system of any one of claims 15 to 19 wherein a tokenised message is generated by a bi-directional communication process.

21. The system of claim 20 wherein the bi-directional communication process is between the token database and an intermediary entity.

22. The system of any one of claims 15 to 21 wherein a step in producing a tokenised message involves de-identifying data.

23. The system of any one of claims 15 to 22 wherein a step in producing a tokenised message involves adding a data element to the message.

24. The system of any one of claims 15 to 23 wherein a step in producing a tokenised message involves removing a data element from the message.

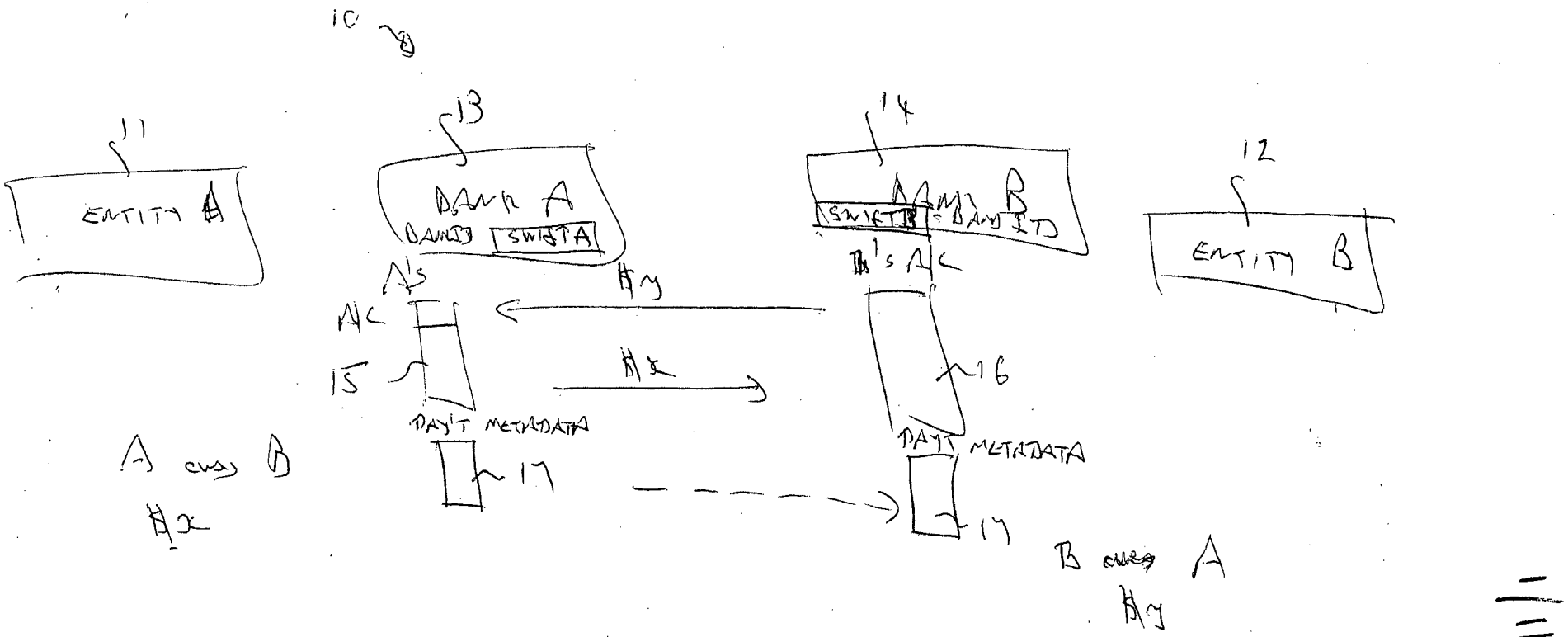
2015903292 14 Aug 2015

25. The system of any one of claims 15 to 24 wherein a step in producing a tokenised message involves applying an algorithm to the data elements in the message.

26. The system of any one of claims 15 to 25 wherein the token database sequences the tokenised messages.

27. The system of any one of claims 15 to 26 wherein the token database sequences the tokenised messages and transmits the tokenised messages as payment data records to a block chain settlement system.

28. The system of claim 27 wherein the block chain settlement system employs the Ripple protocol.



ALT :- any $\Delta(x-y)$

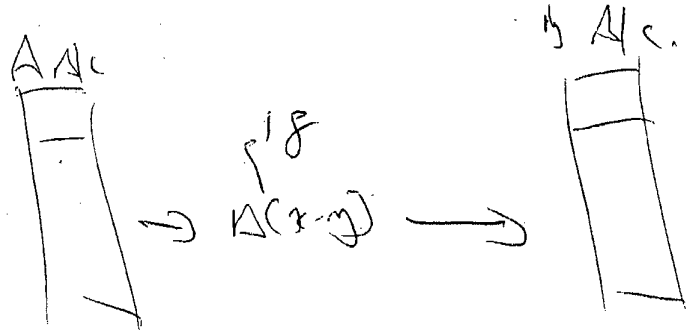


Fig 1A

[Prior Art]

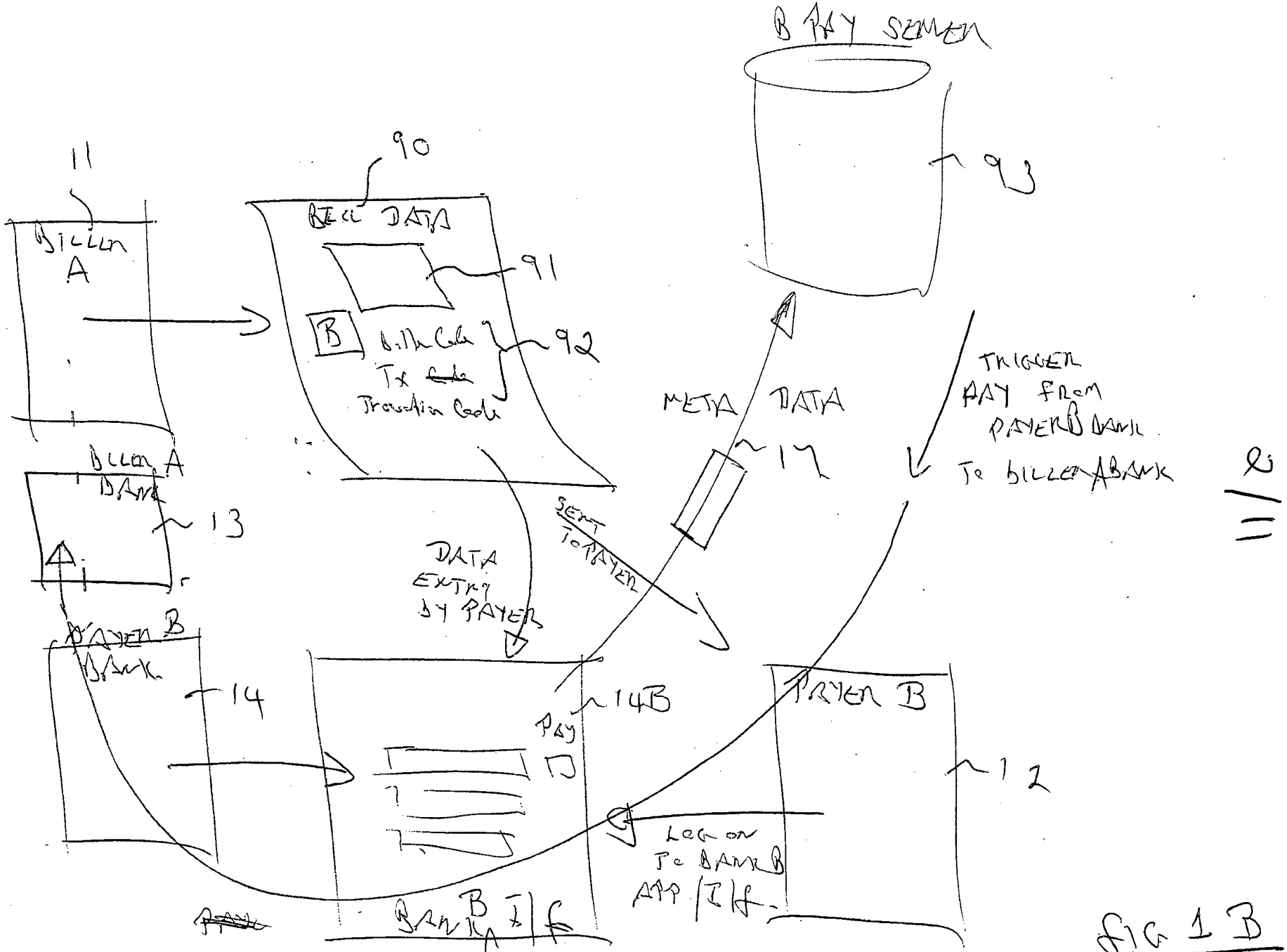
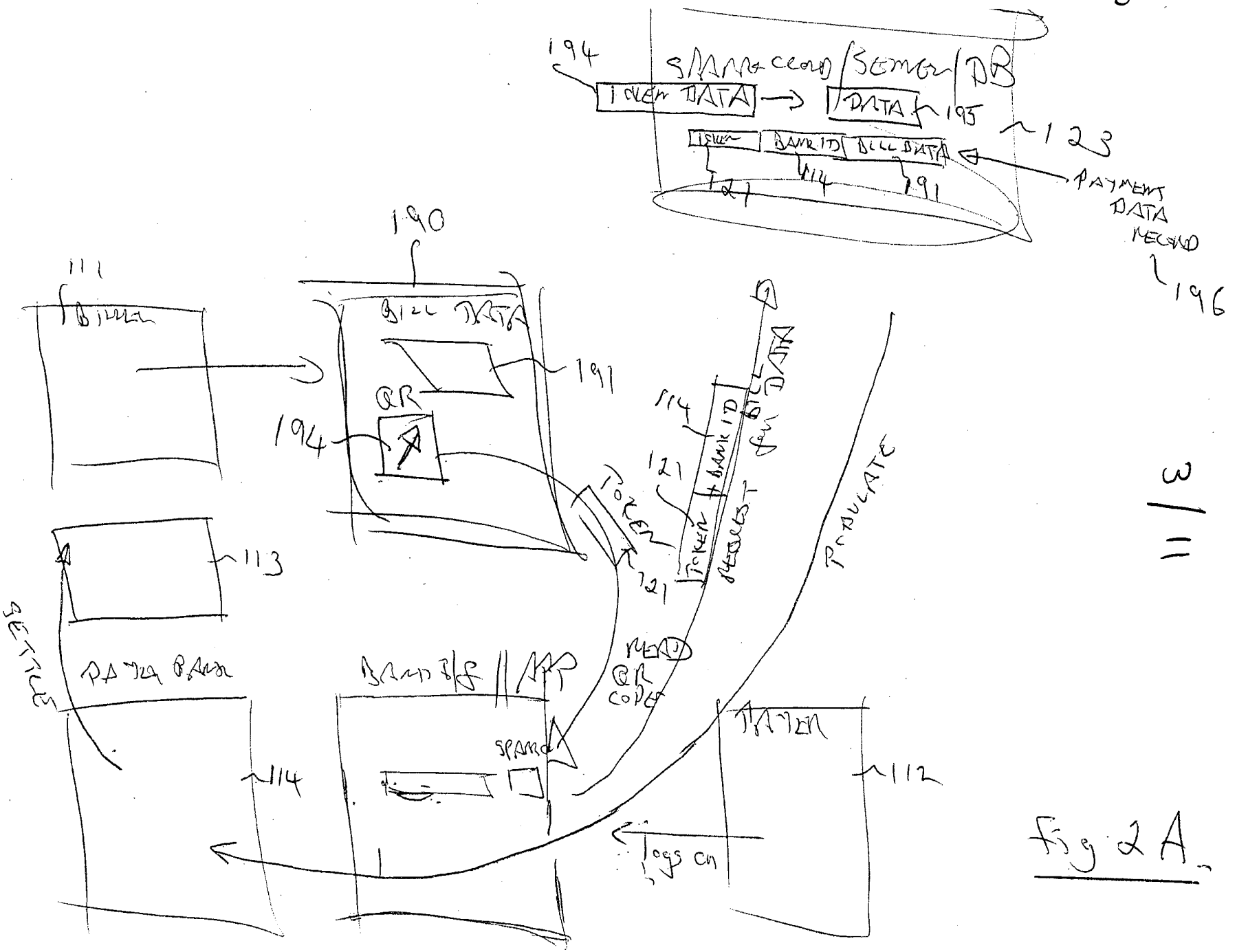

B PAY SERVER
93
11
BILLER A
90
REC DATA
91
B
92
Tx
Transaction Code
BILLER A BANK
13
META DATA
17
TRIGGER PAY FROM PAYER B BANK To BILLER A BANK
8
SENT TO PAYER
DATA ENTRY BY PAYER
PAYER B BANK
14
14B
PAY ID
PAYER B
12
LOG ON To BANK B APP I/F
BANK B I/F

Fig 1B


194
ISSUER DATA
DATA
195
123
ISSUER
BANK ID
BILL DATA
114
191
121
PAYMENT DATA RECORD
196
190
111
BILLER
BILL DATA
191
QR
194
114
121
TOKEN
BANK ID
BILL DATA
REQUEST
PROCESSOR
113
SETTLE
DATA BASE
BANK F/S
APP
RECEIVE QR CODE
SPARE
114
PAYER
112
LOGS ON

3/11

Fig 2A.

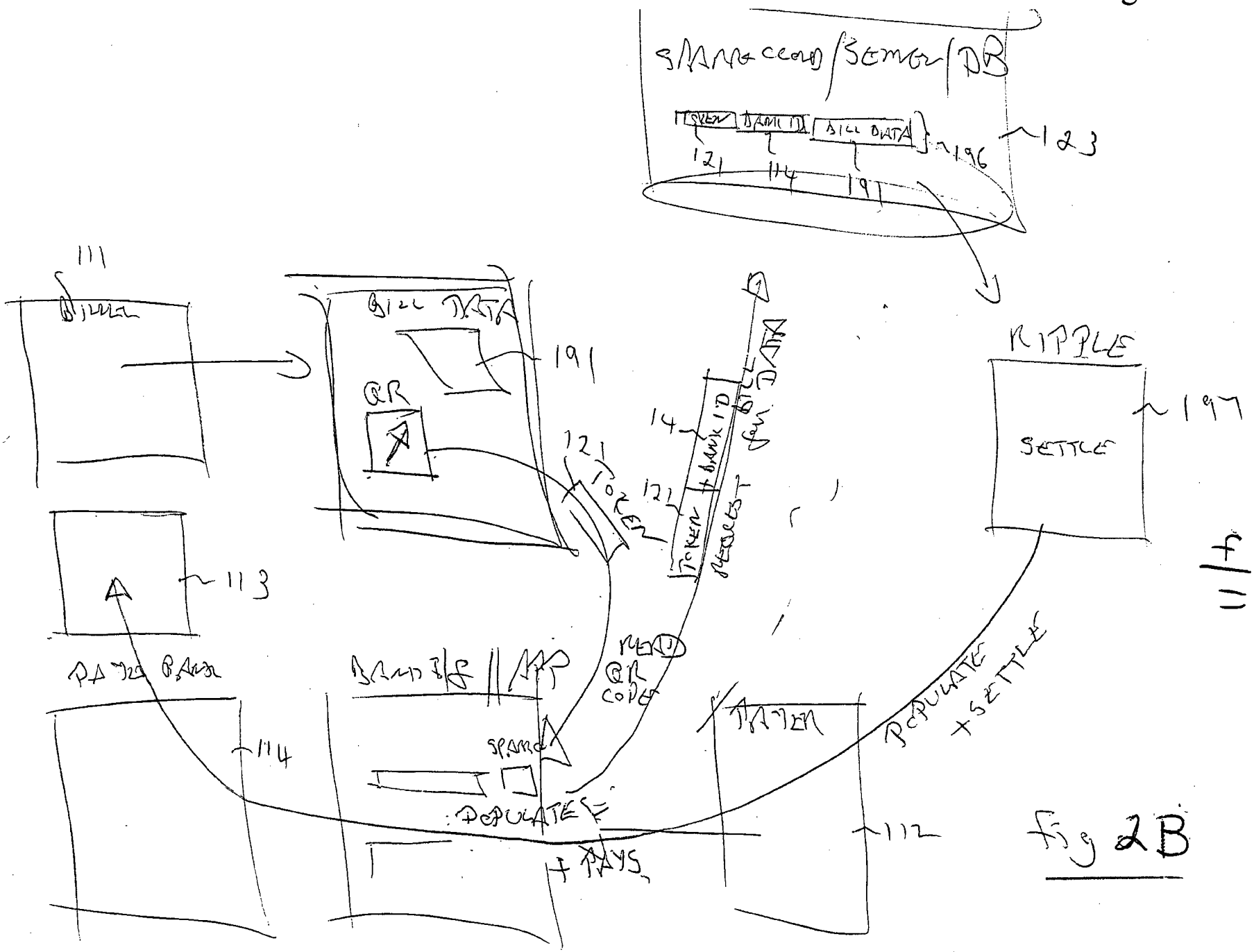

SHARED SERVER DB
SESSION
BANK ID
BILL DATA
121
114
191
196
123
111
BILLER
BILL DATA
191
QR
121
TOKEN
14
BANK ID
BILL DATA
121
TOKEN
REQUEST
RIPPLE
SETTLE
197
113
PAYER BANK
BANK I/F APP
114
QR CODE
SCAN
POPULATE
PAYS
PAYEE
112
POPULATE
+SETTLE

Fig 2B

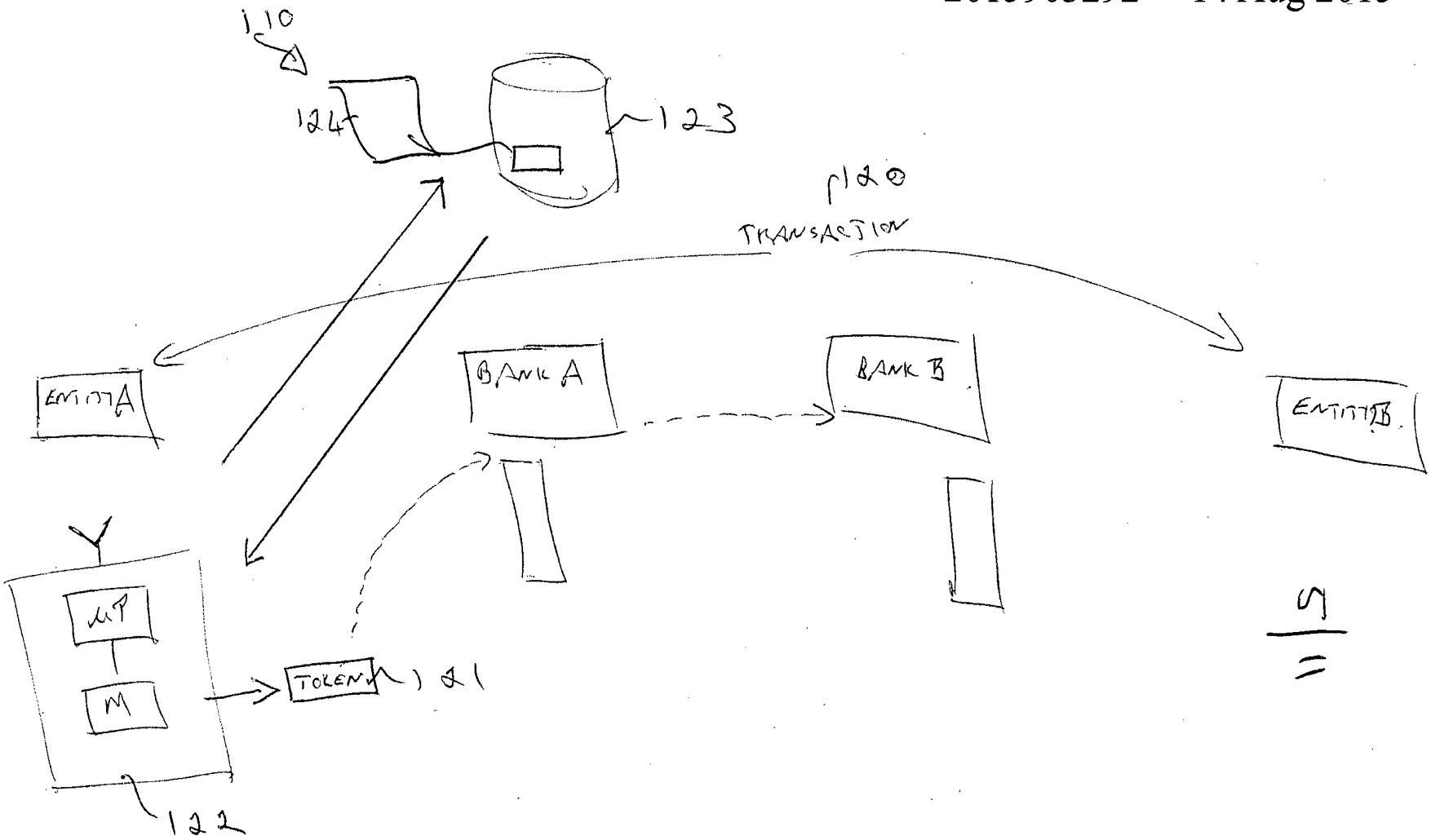


Fig 2 C.

JPMC Ex. 1002
Page 714

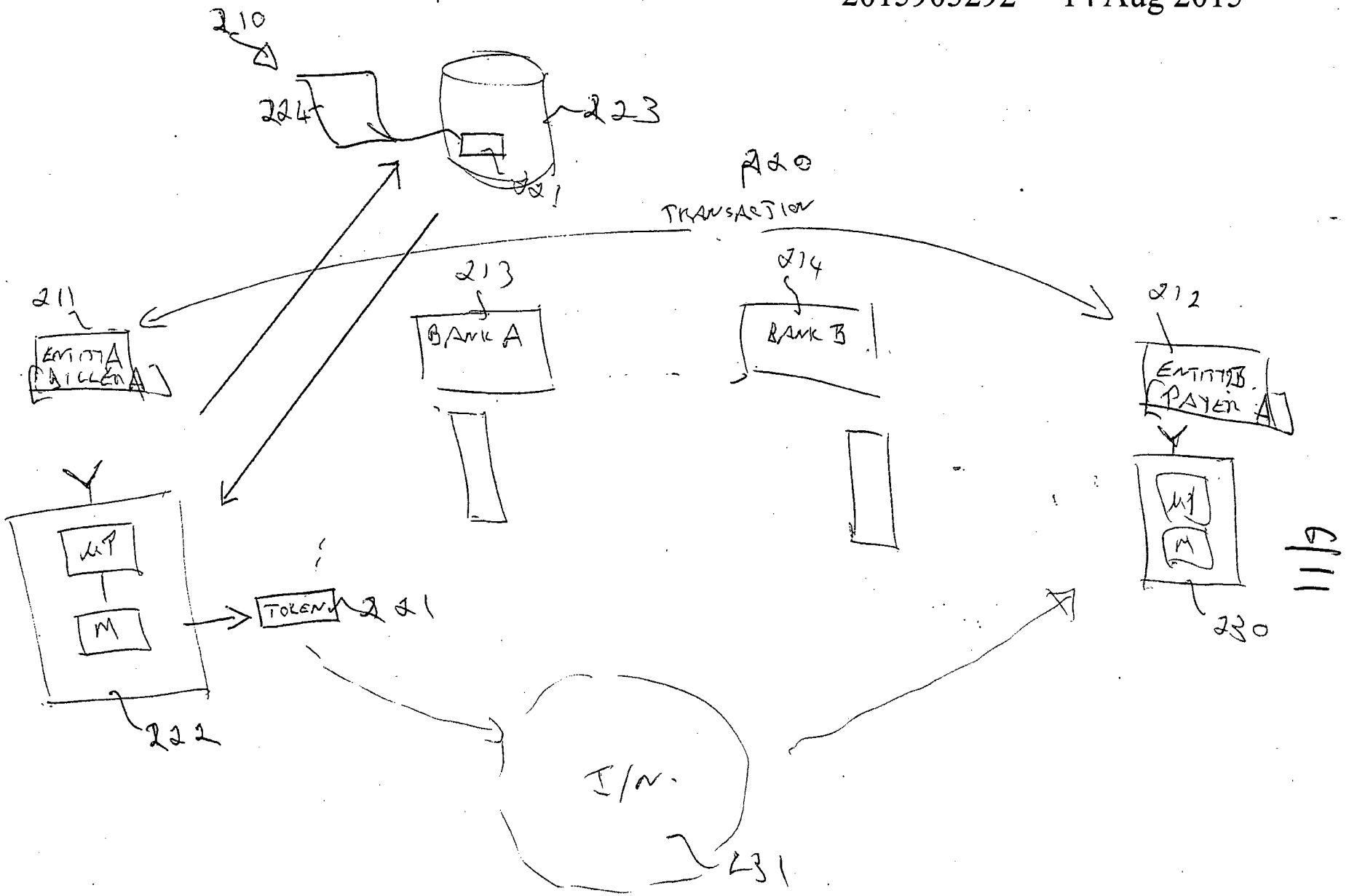

210
224
223
221
220
TRANSACTION
211
ENTITY A
CALLER A
213
BANK A
214
BANK B
212
ENTITY B
PAYER A
MP
M
TOKEN
241
222
I/N.
231
230

Fig 3A

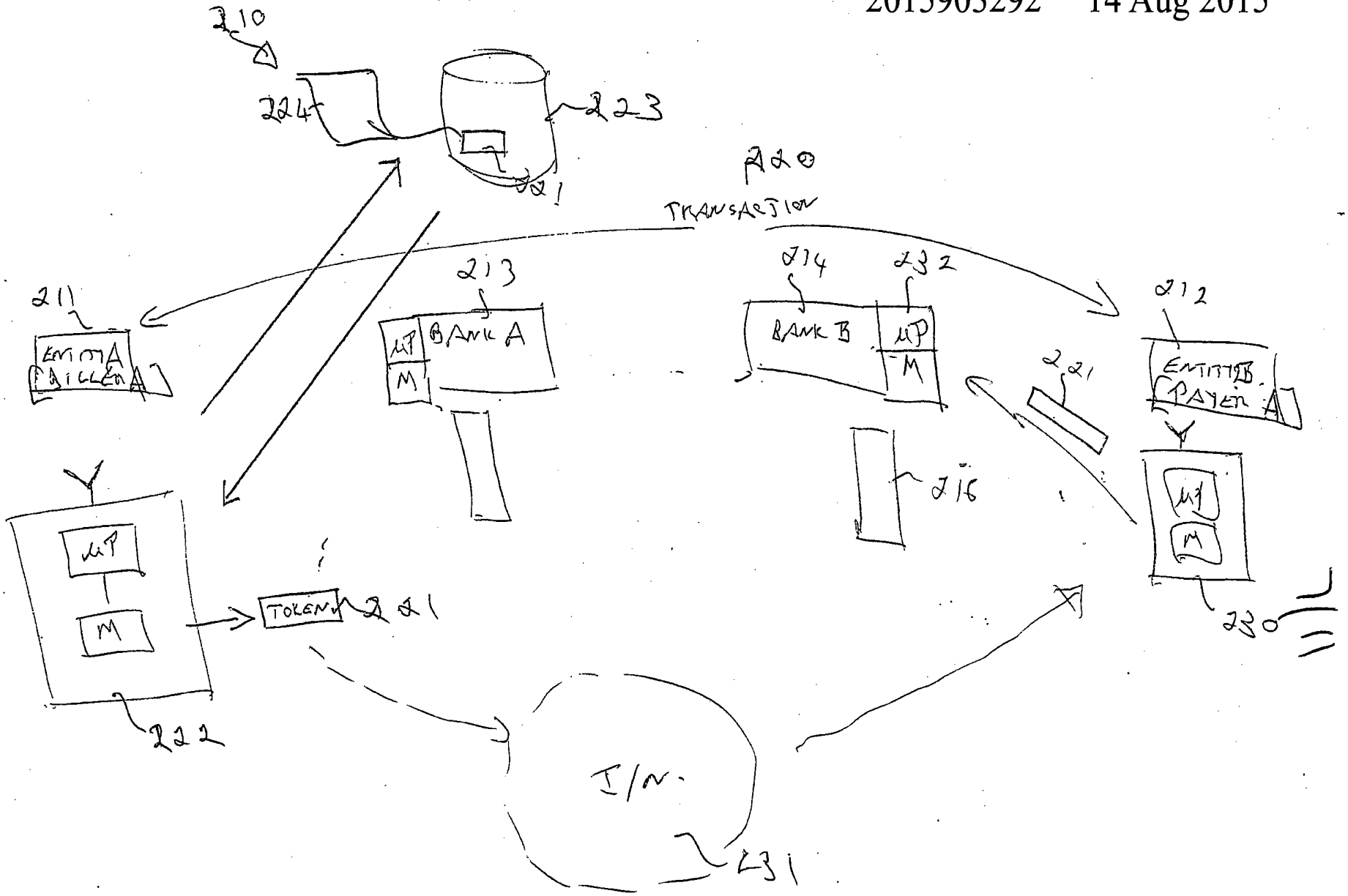

TCR
210
224
223
221
220
TRANSACTION
211
ENTITY A
PAYER A
213
BANK A
MP
M
214
232
BANK B
MP
M
212
ENTITY B
PAYER A
MP
M
221
216
MP
M
TOKEN
241
222
I/N.
231
230

Fig 3B

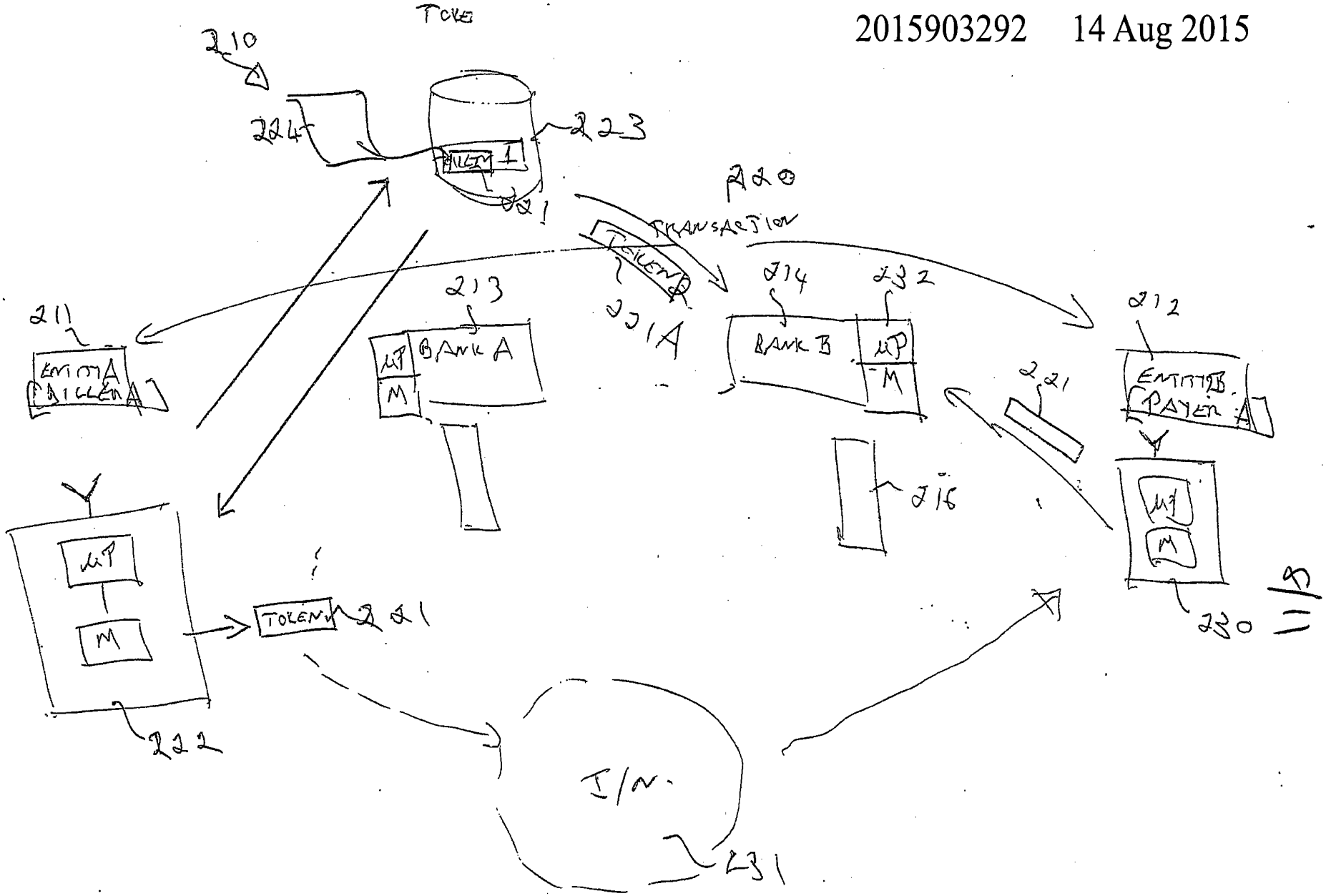
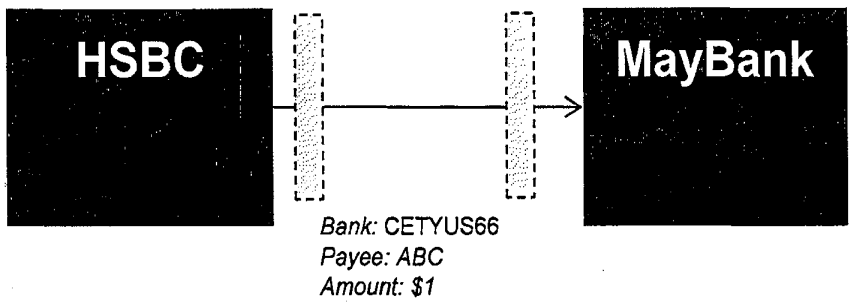

TOKEN
210
224
223
TOKEN 1
221
220
TRANSACTION
TOKEN
231A
211
ENTITY A
CALLER A
213
BANK A
214
232
BANK B
212
ENTITY B
PAYEE A
221
216
TOKEN
241
222
220
I/N.
231

Fig 3C

JPMC Ex. 1002
Page 718

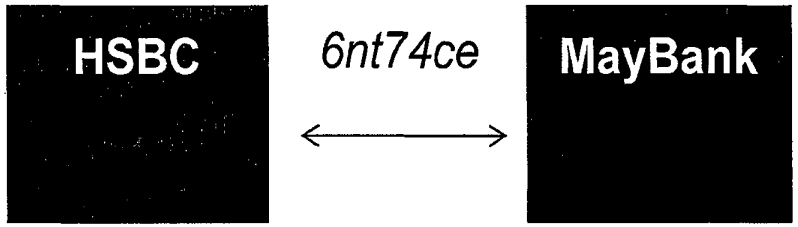
Our token system gives power back to Banks run their own shop; with their own, decentralized security management

Existing (SWIFT) system



(a) Depends on SWIFT infrastructure

Proposed system



(a) Bank-originating (cuts costs)

(b) Optional add-on: Data-enriched for PaaS for customers

14 Aug 2015 20159032 92

JPMC Ex. 1002
Page 719

We can curate our messaging system to accommodate Bank's risk appetite in relation to user data

Base case	Option A: XX	Option B: Data rich
Fully anonymized data	**Text** • Text - Text	**User ID shared with Sparro**
Bank-powered • Tokenization within bank • User ID generation in banks		**Bank-powered** • Tokenization within bank • User ID generation in banks
Benefit • Processing cost • Improved confidentiality of transaction data		**Benefit** • Processing costs • Enriched Payments as a Service to Bank customers

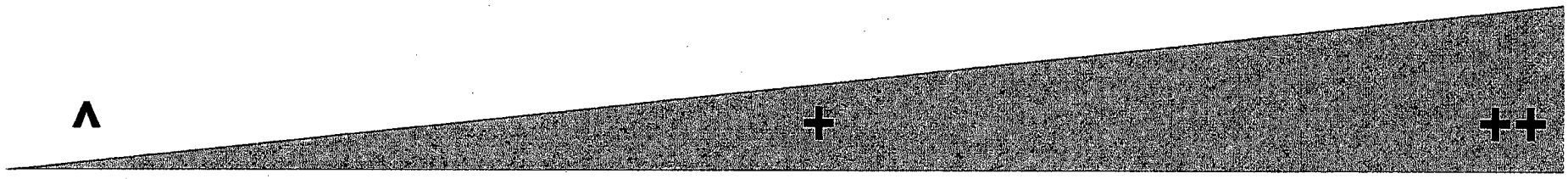


Fig 5

14 Aug 2015 2015903292

SUMMARY: Benefits to Banks vis-a-vis SWIFT and Ripple

Issue	SWIFT	Ripple	Proposed
Commercial	Bypass SWIFT	No competition, given infrastructure focus	1. Banks turn cost centre re SWIFT processing into profit pool 2. *Optional add-on:* new revenue from e.g. PaaS
Security	SWIFT-based	Block chain	1. Bank's private system
Technical	Committed infrastructure spend is slow & expensive	Private gateway establishment	Sparro (anonymized) messaging

fig 6.

WIPO
WORLD
INTELLECTUAL PROPERTY
ORGANIZATION

DOCUMENT MADE AVAILABLE UNDER THE PATENT COOPERATION TREATY (PCT)

International application number:		**PCT/AU2016/000279**
International filing date:		**12 August 2016 (12.08.2016)**
Document type:		**Certified copy of priority document**
Document details:	Country/Office:	**AU**
	Number:	**2015903292**
	Filing date:	**14 August 2015 (14.08.2015)**
Date of receipt at the International Bureau:		**27 September 2016 (27.09.2016)**

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a),(b) or (b-*bis*)

34, chemin des Colombettes
1211 Geneva 20, Switzerland
www.wipo.int

Australian Government IP Australia	Search Information Statement (SIS)	
	Application Number	PCT/AU2016/000279

A. Search Details

Additional Members of the Search Team (if convened):	R. Stopford and M. Van Der Westhuizen	**Earlier Search Results (if available)**	
		Current SIS Completion Date	1 November 2016

B. Search Strategy

Applicant(s)/Inventor(s) name searched in internal databases provided by IP Australia (Nose, Intess)

Espacenet:

240 results found in the Worldwide EN database for: blockchain OR "block chain" in the title, abstract or full text AND 19700101:20150814 as the publication date AND g06 as the IPC classification

31 results found in the Worldwide EN database for: (blockchain OR "block chain") AND document AND (stamp OR token) in the title, abstract or full text AND 19700101:20150814 as the publication date AND g06 as the IPC classification

Google Scholar, keywords:

enrich token Block chain

token Blockchain document combine OR merge OR append OR join

EPOQUE INTERNAL

Database: WPIAP, EPODOC

1		369	AND (/CC/IC G06F OR G06Q OR H04L OR G07C), (OPD<=20150814), (OR BLOCK_CHAIN?, HASH_CHAIN?, (HASH W TREE), (MERKLE W TREE), ((OR LEDGER, REGISTER, REGISTRAR) 4D (OR DISTRIBUTED, ELECTRONIC, OWNERSHIP, DOCUMENT?, TITLE?, CERTIFICATE?, CONTRACT?, TRANSACTION?, FINANCIAL))), (OR ENRICH+, (S (OR COMBIN+, MERG+, APPEND+, JOIN+, CHAIN+), (OR TOKEN?, ATTRIBUT+, HASH+, CHECKSUM?)), STAMP+, TIMESTAMP?, WATERMARK+)

Results of search statement 1 viewed.

Database: TXTE

1		6675	AND (OR BLOCK_CHAIN?, HASH_CHAIN?, (HASH W TREE), (MERKLE W TREE), ((OR LEDGER, REGISTER, REGISTRAR) 4D (OR DISTRIBUTED, ELECTRONIC, OWNERSHIP, DOCUMENT?, TITLE?, CERTIFICATE?, CONTRACT?))), (OR ENRICH+, (S (OR COMBIN+, MERG+, APPEND+, JOIN+, CHAIN+), (OR TOKEN?,HASH+)), TIMESTAMP?)
2	Lim SS 1	359	BLOCK_CHAIN
3	Lim SS 1	1846	TIMESTAMP
4	Lim SS 1	126	3 AND 2

Results of search statement 4 viewed.

In accordance with MPP 4.1.4.1 the 3PT was reconvened upon the completion of the initial search on 26 October 2016.

JPMC Ex. 1002
Page 722

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 February 2017 (23.02.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/027900 A1

(51) **International Patent Classification**:
G06Q 20/38 (2012.01) *G06F 17/30* (2006.01)

(21) **International Application Number**:
PCT/AU2016/000279

(22) **International Filing Date**:
12 August 2016 (12.08.2016)

(25) **Filing Language**: English

(26) **Publication Language**: English

(30) **Priority Data**:

2015903292	14 August 2015 (14.08.2015)	AU
2016900239	27 January 2016 (27.01.2016)	AU
2016901924	20 May 2016 (20.05.2016)	AU

(71) **Applicant**: **IDENTITII PTY LTD** [AU/AU]; Suite 1 Level 3, 66-72 Reservoir St., Surry Hills, New South Wales 2010 (AU).

(72) **Inventors**: **ARMSTRONG, Nick**; Suite 1 Level 3, 66-72 Reservoir St., Surry Hills, New South Wales 2010 (AU). **BUCKINGHAM, Ben**; Suite 1 Level 3, 66-72 Reservoir St, Surry Hills, New South Wales 2010 (AU). **FRIEDMAN, Daniel**; Suite 1 Level 3, 66-72 Reservoir St., Surry Hills, New South Wales 2010 (AU). **SHEPHERD, Elliot**; Suite 1 Level 3, 66-72 Reservoir St, Surry Hills, New South Wales 2010 (AU). **KNIGHT, Eric**; Suite 1 Level 3, 66-72 Reservoir St, Surry Hills, New South Wales 2010 (AU).

(74) **Agent**: **BAXTER PATENT ATTORNEYS PTY LTD**; Suite 2, Level 3A, 1 Bligh St, Sydney, New South Wales 2000 (AU).

(81) **Designated States** *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) **Title**: A COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR

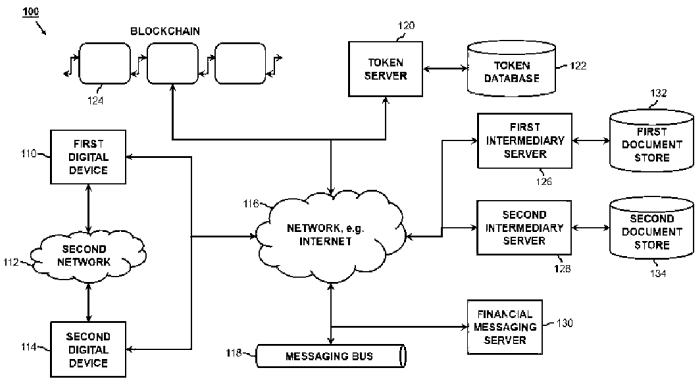


FIG. 1

(57) **Abstract**: The present invention provides a computer implemented method for processing a financial transaction, the method comprising the steps of transmitting one or more documents pertaining to the financial transaction, from a first intermediary server to a first document store, generating an enriched data record from the one or more documents, at the first intermediary server, and adding the enriched data record into a blockchain, from the first intermediary sever, requesting generation of a token corresponding to the financial transaction, to a token server, from the first intermediary server, via a messaging bus, generating the token at the token server and adding the token into the blockchain from the token server, transmitting the token to the first intermediary server from the token server, via the messaging bus and transmitting the token from the first intermediary server to the first document store.

WO 2017/027900 A1

A COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR

Field of the Invention

[001] The present invention relates to financial transactions and in particular to a method and a system for processing a financial transaction.

[002] The invention has been developed primarily for use in/with financial transactions and will be described hereinafter with reference to this application. However, it will be appreciated that the invention is not limited to this particular field of use.

Background of the Invention

[003] A financial transaction comprises at least two parties, with a transfer of currency taking place between the two parties. The currency may include electronic currency and fiat currency. In either case, any financial transaction includes a plurality of data associated with the financial transaction. The plurality of data may include payment metadata such as account numbers of the at least two parties, Business Identifier Codes (BIC) of the financial institutions corresponding to the at least two parties, amount of currency to be transferred and type of currency etc. Further, the plurality of data may include regulatory compliance documents such as KYC documents.

[004] Generally, it is difficult to keep track of the plurality of data during the financial transaction. Further, it is even more difficult to ensure that integrity of the plurality of data is maintained either during or after the financial transaction has been completed or to evidence that it existed at a certain point in the financial transaction process. Many settlement systems are characterised by effective one-way transmission of the plurality of data in any given financial transaction (for example systems based on SWIFT messaging). If it is subsequently discovered that there are deficiencies in the plurality of data transmitted, time consuming checking and querying operations and correspondence often ensues before the financial transaction can be effected.

[005] Therefore there remains, in the art, a need for improved methods and systems for processing a financial transaction which do not suffer from the above mentioned issues.

[006] Any discussion of the background art throughout the specification should in no way be considered as an admission that such background art is prior art, nor that such background art is widely known or forms part of the common general knowledge in the field in Australia or any other country.

Summary of the Invention

[007] According to a first aspect of the present invention, there is provided a computer implemented method for processing a financial transaction, the method comprising the steps of transmitting one or more documents pertaining to the financial transaction, from a first intermediary server to a first document store, generating an enriched data record from the one or more documents, at the first intermediary server, and adding the enriched data record into a blockchain, from the first intermediary sever, requesting generation of a token corresponding to the financial transaction, to a token server, from the first intermediary server, via a messaging bus, generating the token at the token server and adding the token into the blockchain from the token server, transmitting the token to the first intermediary server from the token server, via the messaging bus and transmitting the token from the first intermediary server to the first document store. The token provides a pointer to the enriched data record in the blockchain. Thus the token can used to retrieve the enriched data record at a time of an audit.

[008] In one embodiment of the invention, the computer implemented method further comprises the step of sending a first financial message comprising the token, from the first intermediary server to a second intermediary server, indicative of making a payment to a second user.

[009] In one embodiment of the invention, the computer implemented method further comprises the steps of implementing a smart contract at the token server; and adding the smart contract into the blockchain, from the token server.

[010] In one embodiment of the invention, the computer implemented method further comprises the steps of transmitting the token from the first intermediary server to a first digital device available with a first user, providing the token to a second user, by the first user, providing the token to a second intermediary server, from the second digital device, transmitting the token to a second document store, from the second intermediary server and sending a second financial message comprising the token, from the second intermediary server to the first intermediary server, indicative of making a payment to the first user.

[011] In one embodiment of the invention, the step of generating the enriched data record comprises extracting a plurality of attributes from the one or more documents, at the first intermediary server and combining the plurality of attributes to generate the enriched data record, at the first intermediary server.

[012] In one embodiment of the invention, the step of generating the enriched data record comprises extracting a plurality of attributes from the one or more documents, at the first intermediary server, de-identifying the plurality of attributes to obtain a plurality of de-identified attributes, at the first intermediary server and combining the plurality of de-identified attributes to generate the enriched data record, at the first intermediary server. De-identification of the plurality of attributes ensures that confidentiality of any person or entity involved in the financial transaction is not compromised during a hacking attack on the blockchain.

[013] In one embodiment of the invention, the step of generating the enriched data record comprises extracting a plurality of attributes from the one or more documents, at the first intermediary server, hashing the plurality of attributes to generate a plurality of respective hashes, at the first intermediary server and combining the plurality of hashes to generate the enriched data record, at the first intermediary server. Hashing provides even more protection against tampering of theft, to the one or more documents, as the hashes are irreversible.

[014] In one embodiment of the invention, the computer implemented method further comprises the step of assigning a payment risk rating to the token. The payment risk rating is a direct measure of the regulatory and other compliance checks involved in the financial transaction.

[015] In one embodiment of the invention, the computer implemented method further comprises the steps of transmitting one or more first requests, each comprising the token, from the first intermediary server to the second intermediary server, via the messaging bus, receiving the one or more first requests at the second intermediary server and transmitting the one or more first requests and the token from the second intermediary server to a second document store, generating one or more first responses, each comprising the token, corresponding to the respective one or more first requests, at the second intermediary server, transmitting the one or more first responses from the second intermediary server to the first intermediary server, via the messaging bus, hashing the one or more first requests and the one or more first responses at the second intermediary server to generate one or more first request hashes and one or more first response hashes, respectively, adding the one or more first request hashes and the one or more first response hashes to the enriched data record in the blockchain, from the second intermediary server and receiving the one or more first responses at the first intermediary server and transmitting the one or more first responses to the first document store. This communication between the first intermediary server and the second intermediary server allows the first intermediary server to execute all the necessary compliance checks.

[016] In one embodiment of the invention, the computer implemented method further comprises the steps of hashing the one or more first responses at the first intermediary server to regenerate the one or more first response hashes and verifying the one or more first response hashes with the blockchain from the first intermediary server, using the token. Thus, the integrity of the one or more first responses can be verified with the blockchain, at any given time.

[017] In one embodiment of the invention, each one of the one or more first requests are encrypted with a second public key and signed with a first public

key at the first intermediary server, before transmission to the second intermediary server and decrypted with a second private key at the second intermediary server after reception from the first intermediary server. Further, each one of the one or more first responses are encrypted with the first public key and signed with the second public key at the second intermediary server, before transmission to the first intermediary server and decrypted with a first private key at the first intermediary server after reception from the second intermediary server. Using pairs of asymmetrical keys ensures that the requests and the responses are not intercepted during transmission.

[018] In one embodiment of the invention, the one or more first responses comprise one or more second regulatory compliance documents pertaining to a second user.

[019] In one embodiment of the invention, the computer implemented method further comprises the steps of transmitting one or more second requests, each comprising the token, from the second intermediary server to the first intermediary server, via the messaging bus, receiving the one or more second requests at the first intermediary server and transmitting the one or more second requests from the first intermediary server to the first document store, generating one or more second responses, each comprising the token, corresponding to the respective one or more second requests, at the first intermediary server, transmitting the one or more second responses from the first intermediary server to the second intermediary server, via the messaging bus, hashing the one or more second requests and the one or more second responses at the first intermediary server to generate one or more second request hashes and one or more second response hashes, respectively, adding the one or more second request hashes and the one or more second response hashes to the enriched data record in the blockchain, from the first intermediary server and receiving the one or more second responses at the second intermediary server and transmitting the one or more second responses to the second document store. This communication enables the second intermediary server to execute all the necessary compliance checks.

[020] In one embodiment of the invention, the computer implemented method further comprises the steps of hashing the one or more second responses at the second intermediary server to regenerate the one or more second response hashes and verifying the one or more second response hashes with the blockchain from the second intermediary server, using the token. Similar to one or more first responses, the integrity of the one or more second responses can be verified with the blockchain, at any given time.

[021] In one embodiment of the invention, each one of the one or more second requests are encrypted with a first public key and signed with a second public key at the second intermediary server, before transmission to the first intermediary server and decrypted with a first private key at the first intermediary server after reception from the second intermediary server. Further, each one of the one or more second responses are encrypted with the second public key and signed with the first public key at the first intermediary server, before transmission to the second intermediary server and decrypted with a second private key at the second intermediary server after reception from the first intermediary server. Using pairs of asymmetrical keys ensures that the requests and the responses are not intercepted during transmission.

[022] In one embodiment of the invention, the computer implemented method further comprises the steps of adding the first public key from the first intermediary server into the blockchain and adding the second public key from the second intermediary server into the blockchain.

[023] In one embodiment of the invention, the one or more second responses comprise one or more first regulatory compliance documents pertaining to a first user.

[024] According to a second aspect of the present invention, there is provided a system for processing a financial transaction, the system comprising a first intermediary server operably connected to a network and a first document store, a token server operably connected to the network, a messaging bus operably connected to the network and a blockchain operably connected to the network.

Further, the first intermediary server is configured to transmit one or more documents pertaining to the financial transaction, to the first document store, generate an enriched data record from the one or more documents and add the enriched data record into the blockchain, request generation of a token corresponding to the financial transaction, to the token server, via the messaging bus and transmit the token to the first document store. Further, the token server is configured to generate the token and add the token into the blockchain and transmit the token to the first intermediary server, via the messaging bus.

[025] In one embodiment of the invention, the system further comprises a second intermediary server operably connected to the network and a second document store. Further, the first intermediary server is further configured to send a first financial message comprising the token, to the second intermediary server, indicative of making a payment to a second user.

[026] In one embodiment of the invention, the token server is further configured to implement a smart contract and add the smart contract into the blockchain.

[027] In one embodiment of the invention, the system further comprises a first digital device operably connected to the network, a second digital device operably connected to the network, a second intermediary server operably connected to the network and a second document store. Further, the first intermediary server is further configured to transmit the token to the first digital device. Further, the first digital device comprises a first memory and a first processor operably connected to the first memory, the first memory comprising a first computer program code, the first computer program code when executed by the first processor, instructs the first processor to receive the token from the first intermediary server, provide the token to the second digital device. Further, the second digital device comprises a second memory and a second processor operably connected to the second memory, the second memory comprising a second computer program code, the second computer program code when executed by the second processor, instructs the second processor to receive the token from the first digital device and provide the token to the second intermediary server. Also, the second intermediary server is configured to receive

the token from the second digital device, transmit the token to the second document store and send a second financial message comprising the token, to the first intermediary server, indicative of making a payment to a first user.

[028] In one embodiment of the invention, for generation of the enriched data record, the first intermediary server is configured to extract a plurality of attributes from the one or more documents and combine the plurality of attributes to generate the enriched data record.

[029] In one embodiment of the invention, for generation of the enriched data record, the first intermediary server is configured to extract a plurality of attributes from the one or more documents, de-identify the plurality of attributes to obtain a plurality of de-identified attributes and combine the plurality of de-identified attributes to generate the enriched data record.

[030] In one embodiment of the invention, for generation of the enriched data record, the first intermediary server is configured to extract a plurality of attributes from the one or more documents, hash the plurality of attributes to generate a plurality of respective hashes and combine the plurality of hashes to generate the enriched data record.

[031] In one embodiment of the invention, the first intermediary server is further configured to assign a payment risk rating to the token.

[032] In one embodiment of the invention, the system further comprises a second intermediary server operably connected to the network and a second document store. Further, the first intermediary server is configured to transmit one or more first requests, each comprising the token, to the second intermediary server, via the messaging bus and receive one or more first responses and transmit the one or more first responses to the first document store. Further, the second intermediary server is configured to receive the one or more first requests from the first intermediary server and transmit the one or more first requests and the token to the second document store, generate the one or more first responses, each comprising the token, corresponding to the respective one or more first

requests, transmit the one or more first responses to the first intermediary server, via the messaging bus, hash the one or more first requests and the one or more first responses to generate one or more first request hashes and one or more first response hashes, respectively and add the one or more first request hashes and the one or more first response hashes to the enriched data record in the blockchain.

[033] In one embodiment of the invention, the first intermediary server is further configured to hash the one or more first responses to regenerate the one or more first response hashes and verify the one or more first response hashes with the blockchain, using the token.

[034] In one embodiment of the invention, the first intermediary server is further configured to encrypt each one of the one or more first requests with a second public key and sign each one of the one or more first requests with a first public key, before transmission to the second intermediary server and decrypt each one of the one or more first responses with a first private key after reception from the second intermediary server. Further, the second intermediary server is further configured to encrypt the each one of the one or more first responses with the first public key and sign the each one of the one or more first responses with the second public key, before transmission to the first intermediary server and decrypt the each one of the one or more first requests with a second private key after reception from the first intermediary server.

[035] In one embodiment of the invention, the one or more first responses comprise one or more second regulatory compliance documents pertaining to a second user.

[036] In one embodiment of the invention, the system further comprises a second intermediary server connected to the network and a second document store. Further, the second intermediary server is configured to transmit one or more second requests, each comprising the token, to the first intermediary server, via the messaging bus, receive one or more second responses and transmit the one or more second responses to the second document store. Further, the first

intermediary server is further configured to receive the one or more second requests and transmit the one or more second requests to the first document store, generate the one or more second responses, each comprising the token, corresponding to the respective one or more second requests, transmit the one or more second responses to the second intermediary server, via the messaging bus, hash the one or more second requests and the one or more second responses to generate one or more second request hashes and one or more second response hashes, respectively and add the one or more second request hashes and the one or more second response hashes to the enriched data record in the blockchain.

[037] In one embodiment of the invention, the second intermediary server is further configured to hash the one or more second responses to regenerate the one or more second response hashes and verify the one or more second response hashes with the blockchain, using the token.

[038] In one embodiment of the invention, the second intermediary server is further configured to encrypt each one of the one or more second requests with a first public key and sign each one of the one or more second requests with a second public key, before transmission to the first intermediary server and decrypt each one of the one or more second responses with a second private key after reception from the first intermediary server. Further, the first intermediary server is further configured to encrypt the each one of the one or more second responses with the second public key and sign the each one of the one or more second responses with the first public key, before transmission to the second intermediary server and decrypt the each one of the one or more second requests with a first private key after reception from the second intermediary server.

[039] In one embodiment of the invention, the first intermediary server is further configured to add the first public key into the blockchain and the second intermediary server is further configured to add the second public key into the blockchain.

[040] In one embodiment of the invention, the one or more second responses comprise one or more first regulatory compliance documents pertaining to a first user.

[041] According to a third aspect of the present invention, there is provided a token server for facilitating processing of a financial transaction, operably connected to a network and configured to generate a token, add the token into a blockchain and transmit the token to a first intermediary server, via a messaging bus.

[042] In one embodiment of the invention, the token server is further configured to implement a smart contract and add the smart contract into the blockchain.

[043] According to a fourth aspect of the present invention, there is provided a first intermediary server for facilitating processing of a financial transaction, operably connected to a network and a first document store, and configured to transmit one or more documents pertaining to the financial transaction, to the first document store, generate an enriched data record from the one or more documents and add the enriched data record into a blockchain, request generation of a token corresponding to the financial transaction, to a token server, via a messaging bus and transmit the token to the first document store.

[044] In one embodiment of the invention, the first intermediary server is further configured to send a first financial message comprising the token, to a second intermediary server, indicative of making a payment to a second user.

[045] In one embodiment of the invention, the first intermediary server is further configured to transmit the token to a first digital device.

[046] In one embodiment of the invention, for generation of the enriched data record, the first intermediary server is configured to extract a plurality of attributes from the one or more documents and combine the plurality of attributes to generate the enriched data record.

[047] In one embodiment of the invention, for generation of the enriched data record, the first intermediary server is configured extract a plurality of attributes from the one or more documents, de-identify the plurality of attributes to obtain a plurality of de-identified attributes and combine the plurality of de-identified attributes to generate the enriched data record.

[048] In one embodiment of the invention, for generation of the enriched data record, the first intermediary server is configured to extract a plurality of attributes from the one or more documents, hash the plurality of attributes to generate a plurality of respective hashes and combine the plurality of hashes to generate the enriched data record.

[049] In one embodiment of the invention, the first intermediary server is further configured to assign a payment risk rating to the token.

[050] In one embodiment of the invention, the first intermediary server is further configured to transmit one or more first requests, each comprising the token, to a second intermediary server, via the messaging bus and receive one or more first responses from the second intermediary server and transmit the one or more first responses to the first document store.

[051] In one embodiment of the invention, the one or more first responses comprise one or more second regulatory compliance documents pertaining to a second user.

[052] In one embodiment of the invention, the first intermediary server is further configured to hash the one or more first responses to regenerate one or more first response hashes and verify the one or more first response hashes with the blockchain, using the token.

[053] In one embodiment of the invention, the first intermediary server is further configured to encrypt each one of the one or more first requests with a second public key and sign each one of the one or more first requests with a first public

key, before transmission to the second intermediary server and decrypt each one of the one or more first responses with a first private key after reception from the second intermediary server.

[054] In one embodiment of the invention, the first intermediary server is further configured to receive the one or more second requests from a second intermediary server and transmit the one or more second requests to the first document store, generate one or more second responses, each comprising the token, corresponding to the respective one or more second requests, transmit the one or more second responses to the second intermediary server, via the messaging bus, hash the one or more second requests and the one or more second responses to generate one or more second request hashes and one or more second response hashes, respectively and add the one or more second request hashes and the one or more second response hashes to the enriched data record in the blockchain.

[055] In one embodiment of the invention, the first intermediary server is further configured to encrypt each one of the one or more second responses with a second public key and sign the each one of the one or more second responses with a first public key, before transmission to the second intermediary server and decrypt each one of the one or more second requests with a first private key after reception from the second intermediary server.

[056] In one embodiment of the invention, the first intermediary server is further configured to add the first public key into the blockchain.

[057] According to a fifth aspect of the present invention, there is provided a second intermediary server for facilitating processing of a financial transaction, operably connected to a network and a second document store, and configured to receive the token from the second digital device, transmit the token to the second document store and send a second financial message comprising the token to a first intermediary server, indicative of making a payment to a first user.

[058] According to a sixth aspect of the present invention, there is provided a second intermediary server for facilitating processing of a financial transaction, operably connected to a network and a second document store, and configured to receive one or more first requests, each comprising a token, from a first intermediary server and transmit the one or more first requests and the token to the second document store, generate the one or more first responses, each comprising the token, corresponding to the respective one or more first requests, transmit the one or more first responses to the first intermediary server, via a messaging bus, hash the one or more first requests and the one or more first responses to generate one or more first request hashes and one or more first response hashes, respectively and add the one or more first request hashes and the one or more first response hashes to the enriched data record in the blockchain.

[059] In one embodiment of the invention, the second intermediary server is further configured to encrypt each one of the one or more first responses with a first public key and sign the each one of the one or more first responses with a second public key, before transmission to the first intermediary server and decrypt each one of the one or more first requests with a second private key after reception from the first intermediary server.

[060] According to a seventh aspect of the invention, there is provided a second intermediary server for facilitating processing of a financial transaction, operably connected to a network and a second document store, and configured to transmit one or more second requests, each comprising a token, to a first intermediary server, via a messaging bus and receive one or more second responses from the first intermediary server and transmit the one or more second responses to the second document store.

[061] In one embodiment of the invention, the second intermediary server is further configured to hash the one or more second responses to regenerate one or more second response hashes and verify the one or more second response hashes with the blockchain, using the token.

[062] In one embodiment of the invention, the second intermediary server is further configured to encrypt each one of the one or more second requests with a first public key and sign each one of the one or more second requests with a second public key, before transmission to the first intermediary server and decrypt each one of the one or more second responses with a second private key after reception from the first intermediary server.

[063] In one embodiment of the invention, the second intermediary server is further configured to add the second public key into the blockchain.

[064] In one embodiment of the invention, the one or more second responses comprise one or more first regulatory compliance documents pertaining to a first user.

[065] Other aspects of the invention are also disclosed.

Brief Description of the Drawings

[066] Notwithstanding any other forms which may fall within the scope of the present invention, a preferred embodiment / preferred embodiments of the invention will now be described, by way of example only, with reference to the accompanying drawings in which:

[067] Fig. 1 illustrates a top level diagram of a system of computing devices to which various embodiments described herein may be implemented;

[068] Fig. 2 illustrates a subsystem of the computing devices for generation of a token, in accordance with a preferred embodiment of the present invention;

[069] Fig. 3 illustrates a subsystem of the computing devices for exchange of requests and responses between two intermediary servers, via a messaging bus, in accordance with a preferred embodiment of the present invention;

[070] Fig. 4 illustrates a subsystem of the computing devices for making a payment to a second user, by a first user, in accordance with a preferred embodiment of the present invention;

[071] Fig. 5 illustrates a subsystem of the computing devices for making a payment to the first user, by the second user, in accordance with a preferred embodiment of the present invention;

[072] Fig. 6 illustrates a computing device to which various embodiments described herein may be implemented; and

[073] Fig. 7 illustrates a computer implemented method for processing a financial transaction, in accordance with a preferred embodiment of the present invention;

[074] Figure 8A is a block diagram of the entities and intermediaries involved in a prior art electronic settlement system;

[075] Figure 8B is a data and funds flow according to a prior art settlement system;

[076] Figure 9A, 9B is a data and funds flow diagram according to an indicative embodiment of the present invention;

[077] Figure 9C is a block diagram of the basic infrastructure and components suited for use with embodiments of the present invention;

[078] Figure 10 A, B, C comprise block diagrams of the steps in a settlement transaction in accordance with a first preferred embodiment of the present invention;

[079] Figure 11 is a block diagram of salient characteristics of a messaging system 810 of the prior art as compared with the salient messaging characteristics of the system 1010 enabled by the code of a second embodiment;

[080] Figure 12 illustrates the options for data content to be included in tokens in accordance with embodiments of the invention as described above;

[081] Figure 13 provides a comparison of characteristics of embodiments of the present invention as compared with the prior art Swift-based messaging system;

[082] Figure 14 is a block diagram in accordance with a further preferred embodiment of the present invention;

[083] Figures 15A and15B are block diagrams of an implementation of a blockchain arrangement suitable for use with the system of embodiments of the invention;

[084] Figure 16 is a block diagram in accordance with yet a further preferred embodiment of the present invention and;

[085] Figure 17 is a detailed block diagram of the system of figure 10C and figure 16;

Description of Embodiments

[086] It should be noted in the following description that like or the same reference numerals in different embodiments denote the same or similar features.

System 100 of computing devices

[087] Fig. 1 shows a system 100 of computing devices adapted for implementation of various embodiments of the present invention.

[088] As such, the system 100 comprises a first digital device 110 and a second digital device 114 connected to a network 116. According to various embodiments, the first digital device 110 is one of, but not limited to, a mobile phone, a desktop computer, a laptop or a tablet etc. Similarly, according to various embodiments, the second digital device is one of, but not limited to, a mobile phone, a desktop computer, a laptop or a tablet etc. Further, the network 116 is one of, but not limited to, a Wide Area Network (WAN) or a Local Area

Network (LAN). Preferably the network 116 is internet. The first digital device 110 and the second digital device 114 are also able to communicate through a second network 112. In one embodiment of the invention, the second network 112 is a telecommunication network such as internet or a mobile telecommunication network. In another embodiment, the second network 112 is a non-telecommunication network such as Bluetooth and Near Field Communication (NFC) etc.

[089] Further, the system 100 comprises a first intermediary server 126 and a second intermediary server 128 connected to the network 116. In one embodiment of the invention, the first intermediary server 126 and the second intermediary server 128 represent a first financial institution and a second financial institution, respectively. In one embodiment of the invention, the respective first and second financial institutions are different branches of different of different banks. In another embodiment, the respective first and second financial institutions are different branches of a single bank. In various other embodiments, the respective first and second financial institutions are, but not limited to, commercial banks, investment banks, brokerages, investment companies etc. It is to be noted that each one of the first intermediary server 126 and the second intermediary server 128 may represent a system of servers comprising web servers, application servers, database servers and gateway servers.

[090] Further, the first intermediary server 126 is operably connected to a first document store 132 and the second intermediary server 128 is operably connected to the second document store 134. In one embodiment, the first document store 132 and the second document store 134 represent databases configured to store a plurality of documents. Each one of the documents comprise data pertaining to a financial transaction and metadata corresponding to the data. In various embodiments, metadata comprises format, encoding, author, hash, verification and relationships to other documents.

[091] Further, the system 100 comprises a financial messaging server 130 connected to the network 116. The financial messaging server 130 provides a financial messaging service between any two intermediary servers, including the

first intermediary server 126 and the second intermediary server 128. Some of the examples of financial messaging services include SWIFT (Society for Worldwide Interbank Financial Telecommunication) for cross border transactions. ACH (Automated Clearing House) used in USA and RTGS (Real Time Gross Settlement) used in India and Hong Kong.

[092] Further, the system 100 comprises a token server 120 connected to the network 116 and a token database 122. Further, a blockchain 124 is connected to the network 116. Further, a messaging bus 118 is connected to the network 116. The messaging bus 118 represents a messaging server or a system of messaging servers configured to enable a plurality of applications/servers/devices to communicate with each other. In one embodiment, the messaging bus 118 also comprises an authentication/ authorization server for authorizing the computing devices communicating through the messaging bus 118. The detailed configuration of the messaging bus 118 has been described in the discussion to follow.

[093] Also, a blockchain 124 is connected to the network 116. The configuration and/or the functioning of the first intermediary server 126, the second intermediary server 128, the first document store 132, the second document store 134, the token server 120, the token database 122, the blockchain 124, and the messaging bus 118 has been described below in a description. The system 100 for processing a financial transaction involves subsystems of the computing devices, which have been depicted by means of figures and description as following. The description below has been explained with embodiments comprising a financial transaction between a first user and a second user. In some embodiments, the first user acts as a biller/ beneficiary/payee and the second user acts as purchaser/payer. In other embodiments, the first user acts as a payer and the second user acts as a payee/beneficiary. Further, it is to be noted that the first user and the second user may represent any number of entities involved in the financial transaction.

[094] In one embodiment of the invention, the first user may instruct the first intermediary sever 126 to process the financial transaction. In one embodiment, the financial transaction involves generation of an invoice for the second user

and receiving a payment from the second user, by the first user. In another embodiment, the financial transaction involves making the payment to the second user, by the first user. Specifically, the first user connects with the first intermediary server 126 through the network 116, using the first digital device 110.

[095] Figure 2 illustrates a subsystem (200) of the computing devices for generation of a token, in accordance with a preferred embodiment of the present invention. As shown in figure 2, the first digital device 110 comprises a first processor 210 operably connected to a first memory 220. The first memory 220 comprises a first computer program code, the first computer program code when executed by the first processor 210 instructs the first processor 210 to instruct the first intermediary server 126 to process the financial transaction. Further, in one embodiment of the invention, the first computer program code further instructs the first processor 210 to provide one or more documents pertaining to the financial transaction, to the first intermediary server 126. In another embodiment, the one or more documents are already available with the first intermediary server 126. In yet another embodiment, the first intermediary server 126 is configured to generate at least one document from the one or more documents.

[096] The at least one document may be, but is not limited to, a request for processing the financial transaction. The first intermediary server 126 is configured to transmit the one or more documents pertaining to the financial transaction, to the first document store 132. In one embodiment of the invention, the one or more documents comprise payment metadata such as, but is not limited to, account numbers of the first user (or a beneficiary), Business Identifier Codes (BIC) of the financial institutions corresponding to the first intermediary server 126 and the second intermediary server 128, amount of currency to be transferred and type of currency etc.

[097] Further, in accordance with an embodiment, the one or more documents comprise one or more first regulatory compliance documents pertaining to the first user. Some examples of the regulatory compliance documents include, but are not limited to purpose of payment documents, a result of sanctions screening

and secondary identifiers such as date of birth proof, address proof or other Know Your Customer (KYC) documents.

[098] The first intermediary server 126 is further configured to generate an enriched data record from the one or more documents and add the enriched data record into the blockchain 124. The first intermediary server 126 is configured to generate the enriched data record in multiple ways in multiple embodiments, some of the embodiments have been elucidated below.

[099] In one embodiment of the invention, the first intermediary server 126 is configured to extract a plurality of attributes from the one or more documents. The plurality of attributes may comprise, but are not limited to, originator attributes, beneficiary attributes and purpose of payment etc. Further, the first intermediary server 126 is configured to combine the plurality of attributes to generate the enriched data record. In another embodiment of the present invention, the first intermediary server 126 is configured to extract the plurality of attributes from one or more documents, de-identify the plurality of attributes to obtain a plurality of de-identified attributes and combine the plurality of de-identified attributes to generate the enriched data record. In yet another embodiment of the present invention, the first intermediary server 126 is configured to extract the plurality of attributes from the one or more documents, hash the plurality of attributes to generate a plurality of respective hashes and combine the plurality of hashes to generate the enriched data record.

[0100] Further, the blockchain 124 is a data structure comprising a plurality of blocks of data. Each block of data from the plurality of blocks of data represents a single financial transaction. Further, the blockchain 124 is configured to store data pertaining to the financial transaction in association with the token. The data pertaining to the financial transaction includes, but is not limited to, the enriched data record, a plurality of hashes, a plurality of public keys etc. Also the blockchain 124 is configured to return the data pertaining to the financial transaction, when queried using the token.

[0101] Further, the first intermediary server 126 is configured to request generation of a token, to the token server 120, via the messaging bus 118. The token server

120 in turn is configured to generate the token and add the token into the blockchain 124. The token is stored in the blockchain 124, in association with the enriched data record. Further, the token server 120 is configured to transmit the token to the first intermediary server 126, via the messaging bus 118. Further, the first intermediary server 126 is configured to transmit the token to the first document store 132. The token is stored in the first document store 132, in association with the one or more documents.

[0102] In one embodiment of the invention, the token server 120 is further configured to implement a smart contract and add the smart contract into the blockchain 124. In one embodiment, the smart contract is a shared, signed and verifiable program code which is distributed and/or executed on the blockchain 124. The smart contract would run on the blockchain 124 and would be stored in association with the token.

[0103] In one embodiment of the invention, before proceeding any further, the first intermediary server 126 may wish to perform certain "checks", by communicating with the second intermediary server 128, via the messaging bus 118. For enabling communication, the first intermediary server 126 is configured to generate a first asymmetrical pair of a first public key and a first private key. Further, the first intermediary server 126 is configured to add the first public key and a first address of the first intermediary server 126 into the blockchain 124. Similarly, the second intermediary server 128 is configured to generate a second asymmetrical pair of a second public key and a second private key. Further, the second intermediary server 128 is configured to add the second public key and a second address of the second intermediary server 128 into the blockchain 124.

[0104] Fig. 3 illustrates a subsystem (300) of the computing devices for exchange of requests and responses between the first intermediary server 126 and the second intermediary server 128, via the messaging bus118, in accordance with a preferred embodiment of the present invention. During communication with the second intermediary server 128, the first intermediary server 126 is configured to transmit one or more first requests, each comprising the token, to the second intermediary server 128, via the messaging bus 118. Examples of one or more first requests comprise, but are not limited to, KYC check and payment

acceptance. In one embodiment of the invention, the the one or more first requests are transmitted on basis of a plurality of predefined criterion. For example, if the first intermediary server 126 is required to make the payment to the second intermediary server 128, the first intermediary server 126 may necessitate KYC check of the second user. The second intermediary server 128 is configured to then receive the one or more first requests from the first intermediary server 126 and transmit the one or more first requests and the token to the second document store 134. In one embodiment of the invention, the one or more first requests are transmitted to the second documents store 134 in form of one or more first request documents.

[0105] Further, the second intermediary server 128 is configured to generate one or more first responses, each comprising the token, corresponding to the respective one or more first requests. In one embodiment of the invention, the one or more first responses are generated in form of one or more first response documents at the second intermediary server 128. Further, the second intermediary server 128 is configured to transmit the one or more first responses to the first intermediary server 126, via the messaging bus 118. As an extension of the example above, the second intermediary server 128 may then send a validation successful response to the first intermediary server 126, via the messaging bus 118. In one embodiment of the invention, the one or more first responses comprise one or more second regulatory compliance documents pertaining to a second user.

[0106] Further, the second intermediary server 128 is configured to hash the one or more first requests and the one or more first responses to generate one or more first request hashes and one or more first response hashes, respectively. Also, the second intermediary server 128 is configured to add the one or more first request hashes and the one or more first response hashes to the enriched data record in the blockchain 124. The first intermediary server 126 is then configured to receive the one or more first responses and transmit the one or more first responses to the first document store 132. In one embodiment of the invention, the first intermediary server 126 is further configured to hash the one or more first responses to regenerate the one or more first response hashes. Further, the first intermediary server 126 is configured to verify the one or more first response hashes with the blockchain 124, using the token. The first intermediary server

126 can ensure that the one or more first responses are same as the ones generated at the second intermediary server 128.

[0107] In one embodiment of the invention, to enable secure transmission, the first intermediary server 126 is configured to encrypt each one of the one or more first requests with the second public key and sign each one of the one or more first requests with the first public key, before transmission to the second intermediary server 128. Consequently, the second intermediary server 128 is configured to decrypt the each one of the one or more first requests with the second private key after reception from the first intermediary server 126. In a similar manner, the second intermediary server 128 is configured to encrypt each one of the one or more first responses with the first public key and sign the each one of the one or more first responses with the second public key, before transmission to the first intermediary server 126. Consequently, the first intermediary server 126 is configured to decrypt each one of the one or more first responses with the first private key after reception from the second intermediary server 128.

[0108] The second intermediary server 128 may also request certain compliance checks. Therefore, the second intermediary server 128 is further configured to transmit one or more second requests, each comprising the token, to the first intermediary server 126, via the messaging bus 118. Examples of the one or more second requests comprise, but are not limited to, sender sanctions screening check. The first intermediary server 126 is in turn configured to receive the one or more second requests and transmit the one or more second requests to the first document store 132. In one embodiment of the invention, the one or more second requests are transmitted to the first document store 132 in form of one or more second request documents. Further the first intermediary server 126 is configured to generate one or more second responses, each comprising the token, corresponding to the respective one or more second requests. In one embodiment of the invention, the one or more second responses are generated in form of one or more second response documents. Further, the first intermediary server 126 is configured to transmit the one or more second responses to the second intermediary server 128, via the messaging bus 118. In one embodiment of the invention, the one or more second responses comprise

the one or more first regulatory compliance documents pertaining to the first user.

[0109] Further, the first intermediary server 126 is configured to hash the one or more second requests and the one or more second responses to generate one or more second request hashes and one or more second response hashes, respectively. Further, the first intermediary server 126 is configured to add the one or more second request hashes and the one or more second response hashes to the enriched data record in the blockchain 124. The second intermediary server 128 is in turn configured to receive the one or more second responses and transmit the one or more second responses to the second document store 134. In one embodiment of the invention, the second intermediary server 128 is further configured to hash the one or more second responses to regenerate the one or more second response hashes and verify the one or more second response hashes with the blockchain 124, using the token. Thus ensuring that the one or more second responses are same as those generated at the first intermediary server 126.

[0110] In one embodiment of the invention, to enable secure communication, the second intermediary server 128 is configured to encrypt each one of the one or more second requests with the first public key and sign each one of the one or more second requests with the second public key, before transmission to the first intermediary server 126. Consequently, the first intermediary server 126 is configured to decrypt the each one of the one or more second requests with the first private key after reception from the second intermediary server 128. In a similar manner, the first intermediary server 126 is configured to encrypt each one of the one or more second responses with the second public key and sign the each one of the one or more second responses with the first public key, before transmission to the second intermediary server 128. Consequently, the second intermediary server 128 is configured to decrypt the each one of the one or more second responses with the second private key after reception from the first intermediary server 126.

[0111] The requests and the responses are transmitted in a secure manner across the messaging bus 118, in form of a plurality of messages. It is to be noted that

each one of the plurality of messages comprises a content hash of all its contents to ensure that the contents have not been altered during transmission. The request and/or receipt time of the recipient public key are also attached to the plurality of messages. This ensures only recipient can see message contents & ensures revocability of public keys.

[0112] In one embodiment of the invention, the first intermediary server 128 is further configured to assign a payment risk rating to the token. In one embodiment of the invention, the payment risk rating is assigned to the token at the first intermediary server 126 after completion of the communication with the second intermediary server 128. The payment risk rating provides a pointer to the regulatory and other compliance checks performed by the first intermediary server 126 and the second intermediary server 128. In one embodiment of the invention, the first intermediary server 126 is further configured to add the payment risk rating to the enriched data record in the blockchain 124. Further, the blockchain 124 is configured to return the payment risk rating when queried with the token. The payment risk rating enables better straight through processing by reducing exceptions and false positives.

[0113] The token thus generated may be used to make the payment to the second user by the first user or making the payment to the first user, by the second user. Figure 4 illustrates a subsystem (400) of the computing devices for making the payment to the second user, by the first user. As shown in the figure 4, the first intermediary server 126 is configured to send a first financial message comprising the token, to the second intermediary server 128, indicative of making the payment to the second user. The first financial message is sent through the financial messaging server 130.

[0114] Figure 5 illustrates a subsystem (500) of computing devices for making the payment to the first user, by the second user. As shown in the figure 5, the first intermediary server 126 is further configured to transmit the token to the first digital device 110. In turn, the first computer program code instructs the first processor 210 to receive the token from the first intermediary server 126. In one embodiment of the invention, the first processor 210 is further instructed to provide the token to the second digital device 114 via the network 116 or the

second network 112. The second digital device 110 comprises a second memory 520 and a second processor 510 operably connected to the second memory 520, the second memory 520 comprising a second computer program code, the second computer program code when executed by the second processor 510, instructs the second processor 510 to receive the token from the first digital device 110 and provide the token to the second intermediary server 128.

[0115] In turn the second intermediary server 128 is configured to receive the token from the second digital device 114, transmit the token to the second document store 134 and send a second financial message comprising the token, to the first intermediary server 126, indicative of making the payment to the first user. Further, the second financial message is sent through the financial messaging server 130.

Computing device

[0116] Fig. 56 shows a computing device 600. In a preferred embodiment, the computing device 600 takes the form of the first intermediary server 126, the second intermediary server 128, the token server 120 and the financial messaging server 190 as described above. In this manner, the computing device 500 is adapted to comprise functionality for communication with the network 116, storage capability (such as the token database 122) for storing a plurality of tokens and respective creators of the plurality of tokens.

[0117] However, it should be noted that each one first digital device 110 and the second digital device 114, as shown in figure 1, may also be depicted as the computing device 600. In this manner, the computing device may comprise differing technical integers, such as the display device 6020, one or more human interface devices 660 and the like. In other words, the technical integers of the computing device 500 is shown in figure 5 are exemplary only and variations, adaptations and the like may be made thereto within the purposive scope of the embodiments described herein and having regard for the particular application of the computing device 600.

[0118] In particular the steps of the computer implemented method for processing of a financial transaction, as described in further detail below, may be implemented as computer program code instructions executable by the computing device 600. The computer program code instructions may be divided into one or more computer program code instruction libraries, such as dynamic link libraries (DLL), wherein each of the libraries performs a one or more steps of the computer implemented method. Additionally, a subset of the one or more of the libraries may perform graphical user interface tasks relating to the steps of the computer implemented method.

[0119] The device 600 comprises semiconductor memory 610 comprising volatile memory such as random access memory (RAM) or read only memory (ROM). The memory 600 may comprise either RAM or ROM or a combination of RAM and ROM.

[0120] The device 600 comprises a computer program code storage medium reader 630 for reading the computer program code instructions from computer program code storage media 620. The storage media 620 may be optical media such as CD-ROM disks, magnetic media such as floppy disks and tape cassettes or flash media such as USB memory sticks.

[0121] The device further comprises I/O interface 640 for communicating with one or more peripheral devices. The I/O interface 640 may offer both serial and parallel interface connectivity. For example, the I/O interface 640 may comprise a Small Computer System Interface (SCSI), Universal Serial Bus (USB) or similar I/O interface for interfacing with the storage medium reader 630. The I/O interface 640 may also communicate with the one or more human interface devices (HID) 660 such as keyboards, pointing devices, joysticks and the like. The I/O interface 640 may also comprise a computer to computer interface, such as a Recommended Standard 232 (RS-232) interface, for interfacing the device 600 with one or more personal computer (PC) devices 690. The I/O interface 640 may also comprise an audio interface for communicate audio signals to one or more audio devices 6050, such as a speaker or a buzzer.

[0122] The device 600 also comprises a network interface 650 for communicating with one or more computer networks 680. The network 680 may be a wired network, such as a wired Ethernet™ network or a wireless network, such as a Bluetooth™ network or IEEE 802.11 network. The network 680 may be a local area network (LAN), such as a home or office computer network, or a wide area network (WAN), such as the Internet or private WAN.

[0123] The device 600 comprises an arithmetic logic unit or processor 6000 for performing the computer program code instructions. The processor 6000 may be a reduced instruction set computer (RISC) or complex instruction set computer (CISC) processor or the like. The device 600 further comprises a storage device 6030, such as a magnetic disk hard drive or a solid state disk drive.

[0124] Computer program code instructions may be loaded into the storage device 6030 from the storage media 620 using the storage medium reader 630 or from the network 680 using network interface 650. During the bootstrap phase, an operating system and one or more software applications are loaded from the storage device 6030 into the memory 610. During the fetch-decode-execute cycle, the processor 6000 fetches computer program code instructions from memory 610, decodes the instructions into machine code, executes the instructions and stores one or more intermediate results in memory 600.

[0125] In this manner, the instructions stored in the memory 610, when retrieved and executed by the processor 6000, may configure the computing device 600 as a special-purpose machine that may perform the functions described herein.

[0126] The device 600 also comprises a video interface 6010 for conveying video signals to a display device 6020, such as a liquid crystal display (LCD), cathode-ray tube (CRT) or similar display device.

[0127] The device 600 also comprises a communication bus subsystem 665 for interconnecting the various devices described above. The bus subsystem 665 may offer parallel connectivity such as Industry Standard Architecture (ISA), conventional Peripheral Component Interconnect (PCI) and the like or serial

connectivity such as PCI Express (PCIe), Serial Advanced Technology Attachment (Serial ATA) and the like.

Embodiments of the method

[0128] Figure 7 illustrates a computer implemented method 700 for processing a financial transaction in accordance with an embodiment of the present invention. As described above, the financial transaction is assumed to be taking place between the first user and the second user. The method begins at step 710 by transmitting the one or more documents pertaining to the financial transaction, from the first intermediary server 126 to the first document store 132. In one embodiment of the invention, the one or more documents are provided to the first intermediary server 126 by the first user, from the first digital device 110. In another embodiment, the one or more documents are already available with the first intermediary server 126. In yet another embodiment, the at least one document from the one or more documents is generated at the first intermediary server 126.

[0129] At step 720, the enriched data record is generated from the one or more documents, at the first intermediary server 126. Further, the enriched data record is added into the blockchain 124, from the first intermediary server 126. The enriched data record may be generated in different manners in different embodiments. Some of the embodiments have been discussed below.

[0130] In one embodiment of the invention, the plurality of attributes are extracted from the one or more documents, at the first intermediary server 126. Further, the plurality of attributes are combined to generate the enriched data record at the first intermediary server 126.

[0131] In another embodiment, the plurality of attributes are extracted from the one or more documents, at the first intermediary server 126. Further, the plurality of attributes are de-identified to obtain the plurality of de-identified attributes at the first intermediary server 126. The de-identification of the plurality of attributes comprises removal of any information from the plurality of attributes which may link the plurality of attributes to the first user or the second user. This is to ensure

the confidentiality of the first user and the second user, in case the enriched data record is accessed through illegal routes. The plurality of de-identified attributes are then combined, at the first intermediary server 126, to generate the enriched data record.

[0132] In yet another embodiment, the plurality of attributes are extracted from the one or more documents, at the first intermediary server 126. Further, the plurality of attributes are hashed to generate the plurality of respective hashes, at the first intermediary server 126. The plurality of hashes are then combined to generate the enriched data record, at the first intermediary server 126.

[0133] At step 730, the token server 120 is requested to generate the token corresponding to the financial transaction, from the first intermediary server 126, via the messaging bus 118. At step 740, the token is generated at the token server 120. Further, the token is added into the blockchain 124, from the token server 120. At step 750, the token is transmitted from the token server 120 to the first intermediary server 126. At step 760, the token is transmitted from the first intermediary server 126 to the first document store 132. Further, the token is stored in association with the one or more documents, in the first document store 132.

[0134] In one embodiment of the invention, the smart contract is implemented at the token server 120. Further, the smart contract is added into the blockchain, from the token server 120.

[0135] In one embodiment of the invention, the first intermediary server 126 communicates with the second intermediary server 128, via the messaging bus 118. The communication may take place for verification and validation of the first user and the second user. In one embodiment of the invention, the first asymmetrical pair of the first public key and the first private key is generated at the first intermediary server 126. Further, the first public key and the first address of the first intermediary server 126 are added into the blockchain 124, from the first intermediary server 126. Similarly, the second asymmetrical pair of the second public key and the second private key is generated at the second intermediary server. Further, the second public key and the second address of

the second intermediary server 128 are added into the blockchain 124, from the second intermediary server 128.

[0136] In one embodiment, during communication, the one or more first requests, each comprising the token, are transmitted from the first intermediary server 126 to the second intermediary server 128, via the messaging bus 118. Further, the one or more first requests are received at the second intermediary server 128 and the one or more first requests and the token are transmitted from the second intermediary server 128 to a second document store 134. Further, one or more first responses, each comprising the token, corresponding to the respective one or more first requests, are generated at the second intermediary server 128. Further, the one or more first responses are transmitted from the second intermediary server 128 to the first intermediary server 126, via the messaging bus 118. Further, the one or more first requests and the one or more first responses are hashed at the second intermediary server 128 to generate one or more first request hashes and one or more first response hashes, respectively. Further, the one or more first request hashes and the one or more first response hashes are added to the enriched data record in the blockchain 124, from the second intermediary server 128. Also, the one or more first responses are received at the first intermediary server 126 and transmitted to the first document store 132.

[0137] In one embodiment of the invention, the one or more first responses comprise the one or more second regulatory compliance documents pertaining to the second user. Further, in one embodiment of the invention, the one or more first responses are hashed at the first intermediary server 126 to regenerate the one or more first response hashes. Also, the one or more first response hashes are verified with the blockchain 124 from the first intermediary server 126, using the token.

[0138] In one embodiment of the invention, for secure communication, each one of the one or more first requests are encrypted with the second public key and signed with the first public key at the first intermediary server 126, before transmission to the second intermediary server 128. Consequently, the each one of the one or more first requests are decrypted with the second private key at the

second intermediary server 128 after reception from the first intermediary server 126. Similarly, each one of the one or more first responses are encrypted with the first public key and signed with the second public key at the second intermediary server 128, before transmission to the first intermediary server 126. Also, consequently, the each one of the one or more first responses are decrypted with the first private key at the first intermediary server 126 after reception from the second intermediary server 128.

[0139] Similarly, in the present and various other embodiments, during communication, the one or more second requests, each comprising the token, are transmitted from the second intermediary server 128 to the first intermediary server 126, via the messaging bus 118. Further, the one or more second requests are received at the first intermediary server 126 and the one or more second requests are transmitted from the first intermediary server 126 to the first document store 132. Further, one or more second responses, each comprising the token, corresponding to the respective one or more second requests, are generated at the first intermediary server 126. Further, the one or more second responses are transmitted from the first intermediary server 126 to the second intermediary server 128, via the messaging bus 118. Further, the one or more second requests and the one or more second responses are hashed at the first intermediary server 126 to generate one or more second request hashes and one or more second response hashes, respectively. Further, the one or more second request hashes and the one or more second response hashes are added to the enriched data record in the blockchain 124, from the first intermediary server 126. Also, the one or more second responses are received at the second intermediary server 128 and transmitted to the second document store 134.

[0140] In one embodiment of the invention, the one or more second responses comprise the one or more first regulatory compliance documents pertaining to the first user. Further, in one embodiment, the one or more second responses are hashed at the second intermediary server 128 to regenerate the one or more second response hashes. Also, the one or more second response hashes are verified with the blockchain 124 from the second intermediary server 128, using the token.

[0141] In one embodiment of the invention, for secure communication, each one of the one or more second requests are encrypted with the first public key and signed with the second public key at the second intermediary server 128, before transmission to the first intermediary server 126. Consequently, the each one of the one or more second requests are decrypted with the first private key at the first intermediary server 126 after reception from the second intermediary server 128. Similarly, each one of the one or more second responses are encrypted with the second public key and signed with the first public key at the first intermediary server 126, before transmission to the second intermediary server 128, and decrypted with the second private key at the second intermediary server 128 after reception from the first intermediary server 126.

[0142] In one embodiment of the invention, the payment risk rating is assigned to the token, at the first intermediary server 126. Further, the payment risk rating is added to the enriched data record in the blockchain 124, from the first intermediary server 126.

[0143] In one embodiment, for making the payment to second user, by the first user, the first financial message comprising the token, is sent from the first intermediary server 126 to the second intermediary server 128, indicative of making the payment to the second user. Further, the first financial message is sent via the financial messaging server 130.

[0144] In another embodiment, the token is transmitted from the first intermediary server 126 to the first digital device 110, available with the first user. The first processor 210 receives the token from the first intermediary server 126 and stores the token in the first memory 220. Further, the token is provided to the second user, by the first user. In one embodiment, the token is provided to the second user by means of a Quick Response (QR) code printed on an invoice. In another embodiment, the token is provided to the second user at the second digital device 114 available with the second user, from the first digital device 110. The second processor 510 receives the token from the first digital device 110, and stores the token in the second memory 520.

[0145] Further, the token is provided to the second intermediary server 128, from the second digital device 114, by the second user. The second computer program code instructs the second processor 510 to provide the token to the second intermediary server. The token is then transmitted to the second document store 134, from the second intermediary server 128. Further, the second financial message is sent from the second intermediary server 128, to the first intermediary server 126, indicative of making the payment to the first user.

Prior Art

[0146] With reference to Figure 8A there is illustrated in block form the basic components of a prior art settlement system. In many transactions there will be an at least first transacting entity 811 which enters into a financial transaction with an at least second transacting entity 812. The financial transaction may be as simple as the agreement by the first transacting entity 811 to sell a particular item or service to the second transacting entity 812. Typically the financial transaction will require settlement for an agreed amount expressed in a Fiat or other currency. In the vast majority of cases the at least first transacting entity 811 will be associated with an at least first intermediary entity 813, in this instance in the form of a bank A and similarly the second transacting entity 812 will be associated with an at least second intermediary entity 814 in this instance in the form of bank B. The first transacting entity 811 will have a first bank account 815 at the first intermediary entity 813 whilst second transacting entity 812 will have a second bank account 816 at second intermediary entity 814. Settlement of any given transaction requires instruction given by first transacting entity 811 to its first intermediary entity 813 to pay an agreed amount from the first bank account 815 to the bank account comprising second bank account 816 of second intermediary entity 814 of second transacting entity 812. For these instructions to be carried out metadata in the form of payment metadata 817 must be assembled at the first intermediary entity 813 sufficient and exhaustive to communicate to the second intermediary entity 814 such that the agreed settlement amount is transmitted from bank A to bank B and more particularly to the specific accounts of the respective first transacting entity 811 and second transacting entity 812.

[0147] A similar transaction may be applied in reverse where the second transacting entity sells a good or service to first transacting entity 811. In such an instance the respective intermediaries, once having received the respective payment metadata 817 and exchanged that metadata 817 may elect to simply pay the difference 818 electronically as between the intermediaries to effect the multiple transactions. In some instances, particularly where the financial transaction is cross-border-for example the first intermediary entity 813 is in a first country whilst the second intermediary entity 814 is in a second country the metadata 817 may include what is known as a Swift code which is a substantially unique identifier for each intermediary entity involved in the financial transaction. However, for any given transaction, far more data than merely a unique identifier for each intermediary entity involved in a financial transaction is required in order for the appropriate settlement amounts to ultimately be recorded in the correct accounts and settle the financial transaction for the agreed amounts.

[0148] Figure 8B is a data and funds flow diagram of data and funds flow according to a prior art settlement system at the granular level. In this instance, with reference to figure 8B like components are numbered as for figure 8A a given transaction requiring settlement can be embodied as a bill 890 which will include payment data 891 and may include bank facilitation payment data 892 comprising, in this instance, a biller code and a financial transaction code. Banks which are party to this bank facilitation payment system permit data entry by entity B (or payer B) 812 into a database of bank B 814 by means of a bank application or web interface 814 B. Bank B may then add additional data to form metadata 817 which is sent to a third-party server 893 which utilises metadata 817 to trigger pay (settlement) of bill 890 from payer B bank 814 to biller A bank 813.

Exemplary Embodiments

[0149] With reference to Figure 9C there is illustrated a block diagram of the basic infrastructure and components suited for use with embodiments of the present invention. In this instance like components are numbered as for figure 8 except in the 900 series. So, for example, first transacting entity 811 becomes first transacting entity 911 in this embodiment with reference to figure 2C

[0150] In this instance a settlement system 910 according to a generalised embodiment includes at least first transacting entity 911 which enters into a financial transaction with at least a second transacting entity 912. As previously these entities are associated with a respective first intermediary entity 913 and a second intermediary entity 914 in the form of bank A and bank B. Each of the first transacting entity 911 and a second transacting entity 912 has a respective account 915, 916 at their respective intermediary entities as illustrated in figure 9C

[0151] In this instance, in the event that first transacting entity 911 enters into a financial transaction with second transacting entity 912 then, at the time of entry into the financial transaction 920, a token 921 is generated. In this instance the token 921 is generated by at least first digital device 922 communicating with a token database 923. The token database 923 generates a token comprising a data file 924 containing all data that will ultimately be required to settle the financial transaction 920 including any necessary identifying information for the transacting entity is, their accounts and the intermediary entities. Settlement is effected by communication of the token 921 to bank A and then to bank B together with the appropriate flow of funds.

[0152] With reference to figure 9A at the granular level a bill 990 from a biller 911 directed to a payer 912 contains bill data 991 and also token data of a token 921 residing within a code symbol 994 (in this instance a QR code). The token data includes pointer data pointing to data 995 on token database 923. The data 995 combined with bank ID data 914 permits the creation by token database 923 of a full payment record 996 which can be utilised to cause settlement of the bill 990 as against payer 912 via, in this instance, their respective banks 914, 913.

[0153] With reference to figure 9B the payment data record 996 is utilised has fed into a settlement network such as, for example a network 997 operating under the Ripple protocol thereby permitting substantially real-time settlement across multiple institutions and banks.

[0154] With reference to Figures 10 there is illustrated in block diagram form a first preferred embodiment of the present invention by way of a non-limiting example of a financial transaction. In this embodiment like components are numbered as for the previous embodiments except in the 1000 series. So, for example, token 921 becomes token 1021.

[0155] With reference to figure 10A the financial transaction system 1010 is activated, as for the previous embodiment, when a financial transaction 1020 is entered into between at least first transacting entity 1011 and at least a second transacting entity 1012 each dealing, for the purposes of this transaction, through respective intermediary entities 1013, 1014.

[0156] At the time of and as part of entry into the financial transaction 1020 the first transacting entity 1011 accesses token database 1023 via digital device 1022 executing via a web browser interface or via execution of an application running on a portable digital devices such as a mobile telephone or in a further alternative as a point-of-sale terminal in order to arrange for the database 1023 to generate a token 1021. In this instance the token 1021 will include better data 1024 including the recipient named, BIC, IBAN, destination country, mobile number, currency, business type, communication, payment amount. In this instance the token 1021 including the metadata 1024 is stored in the token database 1023. In addition the first transacting entity 1011 communicates the token 1021 to a digital device 1030 associated with second transacting entity 1012. In this instance the communication is by way of initial transmission of the token 1021 to digital device 1022 which then on transmits the token via Internet 1031 to digital device 1030.

[0157] With reference to figure 10B, when ready to settle the financial transaction 1020 the second transacting entity 1012 "logs in" to a portal associated with second intermediary entity 1014 and communicates the token 1021. In this instance have the login can be executed via a web browser associated with digital device 1030 which communicates via Internet 1031 the token 1021 to a digital processing system 1032 (including at least a processor and a memory) associated with second intermediary entity 1014. Substantially at the same time as part of seeking to settle the financial transaction 1020:

[0158] Notification: token database 1023 notifies second intermediary entity 1014 to contact the token database 1023 from which it receives a further token 1021A.

[0159] Verification: token database 1023 communicates with the processing system 1032 of second intermediary entity 1014 to verify that sufficient funds are located in account 1016 as indicated in the meta data 1024 to settle the financial transaction.

[0160] Committing payer funds: payers bank debits payers account: payers bank sends notice to payer bank gateway: payers bank gateway calls token database 1023 to get approved token:

[0161] Settlement: gateway of payers bank sends by way of non-limiting example XRP (the native currency of the Ripple protocol) to billers bank gateway: payers bank gateway notifies token database 1023 of receipt:

[0162] Clearing: payer's bank Nostro account is debited subject to bank institution rules.

[0163] Examples of tokenised messages and their generation and transmission are illustrated in pseudocode below. Reference to "sparro" is a reference to an instance of a token databasep23.

[0164] The previous, meta-data mode is first. It switches to minimal half way through

[0165] --

[0166] Bank:HSBC >> createUserCode >> Sparro:Sparro

[0167] {"id":"User:ABC Paper","name":"ABC Paper"}

[0168] (Creating Sparro User Code - Meta-data given can be used by other banks for compliance and for confirming payee with customers.)

[0169] --

[0170] Bank:MayBank >> createUserCode >> Sparro:Sparro

[0171] {"id":"User:XYZ Printing","name":"XYZ Printing"}

[0172] (Creating Sparro User Code - Meta-data given can be used by other banks for compliance and for confirming payee with customers.)

[0173] --

[0174] Sparro:Sparro >> createUserCode-reply >> Bank:HSBC

[0175] {"id":"User:ABC Paper","name":"ABC Paper","code":"65q3gdd"}

[0176] --

[0177] Sparro:Sparro >> createUserCode-reply >> Bank:MayBank

[0178] {"id":"User:XYZ Printing","name":"XYZ Printing","code":"70wqgx6"}

[0179] --

[0180] User:ABC Paper >> createInvoice >> Bank:HSBC

[0181] {"amount":{"amount":1000,"currency":"gbp"}}

[0182] --

[0183] Bank:HSBC >> createInvoiceCode >> Sparro:Sparro

[0184] {"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd"}

[0185] (Creating Invoice Code - An invoice code is created by Sparro and connected to the bank.)

[0186] -

[0187] Sparro:Sparro >> createInvoiceCode-reply >> Bank:HSBC

[0188] {"code":"6tq6wcbad"}

[0189] --

[0190] Bank:HSBC >> createInvoice-reply >> User:ABC Paper

[0191]
{"invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

[0192] Abc invoice { amount: { amount: 1000, currency: 'gbp' },

[0193] payee: '65q3gdd',

[0194] code: '6tq6wcbad' }

[0195] --

[0196] User:ABC Paper >> invoice >> User:XYZ Printing

[0197]
{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}

[0198] -

[0199] User:XYZ Printing >> payInvoice >> Bank:MayBank

[0200] {"invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300}}

[0201] --

[0202] Bank:MayBank >> sendMoney >> BankGateway:MayBank

[0203]

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300}}

[0204] --

[0205] BankGateway:MayBank >> getInvoice >> Sparro:Sparro

[0206] "6tq6wcbad"

[0207] (Sending Payment to Invoice - The payment is sent to the bank that created the invoice.)

[0208] --

[0209] Sparro:Sparro >> getInvoice-reply >> BankGateway:MayBank

[0210]

{"bank":"Bank:HSBC","invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

[0211] --

[0212] BankGateway:MayBank >> transfer >> BankGateway:HSBC

[0213]

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":"ripple-1"}

[0214] --

[0215] BankGateway:HSBC >> incomingTransfer >> Bank:HSBC

[0216]

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":"ripple-1"}

[0217] --

[0218] BankGateway:HSBC >> transfer-reply >> BankGateway:MayBank

[0219] {"success":true,"owed":{"GBP":300}}

[0220] --

[0221] Bank:HSBC >> getInvoice >> Sparro:Sparro

[0222] "6tq6wcbad"

[0223] --

[0224] BankGateway:MayBank >> sendMoney-reply >> Bank:MayBank

[0225]

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":"ripple-1"}

[0226] --

[0227] Sparro:Sparro >> getInvoice-reply >> Bank:HSBC

[0228]

{"bank":"Bank:HSBC","invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

[0229] --

[0230] Bank:MayBank >> payInvoice-reply >> User:XYZ Printing

[0231]

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":"ripple-1"}

[0232] XYZ part-paid invoice {

[0233] "payer": "70wqgx6",

[0234] "invoice": "6tq6wcbad",

[0235] "amount": {

[0236] "currency": "GBP",

[0237] "amount": 300

[0238] },

[0239] "id": "ripple-1"

[0240] }

[0241] --

[0242] Bank:HSBC >> incomingTransfer >> User:ABC Paper

[0243]

{"invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"},"transfer":{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":300},"id":"ripple-1"}}

[0244] -

[0245] User:XYZ Printing >> payInvoice >> Bank:MayBank

[0246] {"invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700}}

[0247] --

[0248] Bank:MayBank >> sendMoney >> BankGateway:MayBank

[0249]

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700}}

[0250] --

[0251] BankGateway:MayBank >> getInvoice >> Sparro:Sparro

[0252] "6tq6wcbad"

[0253] (Sending Payment to Invoice - The payment is sent to the bank that created the invoice.)

[0254] --

[0255] Sparro:Sparro >> getInvoice-reply >> BankGateway:MayBank

[0256]

{"bank":"Bank:HSBC","invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

[0257] --

[0258] BankGateway:MayBank >> transfer >> BankGateway:HSBC

[0259]

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700},"id":"ripple-2"}

[0260] --

[0261] BankGateway:HSBC >> incomingTransfer >> Bank:HSBC

[0262]

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700},"id":"ripple-2"}

[0263] --

[0264] BankGateway:HSBC >> transfer-reply >> BankGateway:MayBank

[0265] {"success":true,"owed":{"GBP":1000}}

[0266] --

[0267] Bank:HSBC >> getInvoice >> Sparro:Sparro

[0268] "6tq6wcbad"

[0269] -

[0270] BankGateway:MayBank >> sendMoney-reply >> Bank:MayBank

[0271]

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700},"id":"ripple-2"}

[0272] --

[0273] Sparro:Sparro >> getInvoice-reply >> Bank:HSBC

[0274]

{"bank":"Bank:HSBC","invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"}}

[0275] --

[0276] Bank:MayBank >> payInvoice-reply >> User:XYZ Printing

[0277]

{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700},"id":"ripple-2"}

[0278] XYZ finished paying invoice {

[0279] "payer": "70wqgx6",

[0280] "invoice": "6tq6wcbad",

[0281] "amount": {

[0282] "currency": "GBP",

[0283] "amount": 700

[0284] },

[0285] "id": "ripple-2"

[0286] }

[0287] --- SWITCHING TO MODE: minimal ---

[0288] --

[0289] Bank:HSBC >> incomingTransfer >> User:ABC Paper

[0290]

{"invoice":{"amount":{"amount":1000,"currency":"gbp"},"payee":"65q3gdd","code":"6tq6wcbad"},"transfer":{"payer":"70wqgx6","invoice":"6tq6wcbad","amount":{"currency":"GBP","amount":700},"id":"ripple-2"}}

[0291] --Bank:HSBC >> createUserCode >> Sparro:Sparro

[0292] undefined

[0293] (Creating Sparro User Code - No meta-data is required.)

[0294] --

[0295] Bank:MayBank >> createUserCode >> Sparro:Sparro

[0296] undefined

[0297] (Creating Sparro User Code - No meta-data is required.)

[0298] --

[0299] Sparro:Sparro >> createUserCode-reply >> Bank:HSBC

[0300] {"code":"dnt7gec"}

[0301] --

[0302] Sparro:Sparro >> createUserCode-reply >> Bank:MayBank

[0303] {"code":"6wwpwuc"}

[0304] --

[0305] User:ABC Paper >> createInvoice >> Bank:HSBC

[0306] {"amount":{"amount":2000,"currency":"gbp"}}

[0307] --

[0308] Bank:HSBC >> createInvoiceCode >> Sparro:Sparro

[0309] null

[0310] (Creating Invoice Code - An invoice code is created by Sparro and connected to the bank. No invoice details are required.)

[0311] --

[0312] Sparro:Sparro >> createInvoiceCode-reply >> Bank:HSBC

[0313] {"code":"erwkax1md"}

[0314] --Bank:HSBC >> createInvoice-reply >> User:ABC Paper

[0315]

{"invoice":{"amount":{"amount":2000,"currency":"gbp"},"code":"erwkax1md","payee":"User:ABC Paper","transfers":[]}}

[0316] Abc invoice { amount: { amount: 2000, currency: 'gbp' },

[0317] code: 'erwkax1md',

[0318] payee: 'User:ABC Paper',

[0319] transfers: [] }

[0320] --

[0321] User:ABC Paper >> invoice >> User:XYZ Printing

[0322]

{"amount":{"amount":2000,"currency":"gbp"},"code":"erwkax1md","payee":"User:ABC Paper","transfers":[]}

[0323] --

[0324] User:XYZ Printing >> payInvoice >> Bank:MayBank

[0325] {"invoice":"erwkax1md","amount":{"currency":"GBP","amount":600}}

[0326] --

[0327] Bank:MayBank >> sendMoney >> BankGateway:MayBank

[0328]

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600}}

[0329] --

[0330] BankGateway:MayBank >> getInvoice >> Sparro:Sparro

[0331] "erwkax1md"

[0332] (Sending Payment to Invoice - The payment is sent to the bank that created the invoice.)

[0333] --

[0334] Sparro:Sparro >> getInvoice-reply >> BankGateway:MayBank

[0335] {"bank":"Bank:HSBC"}

[0336] --

[0337] BankGateway:MayBank >> transfer >> BankGateway:HSBC

[0338]

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}

[0339] --

[0340] BankGateway:HSBC >> incomingTransfer >> Bank:HSBC

[0341]

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}

[0342] --

[0343] BankGateway:HSBC >> transfer-reply >> BankGateway:MayBank

[0344] {"success":true,"owed":{"GBP":600}}

[0345] --

[0346] Bank:HSBC >> incomingTransfer >> User:ABC Paper

[0347]

{"invoice":{"amount":{"amount":2000,"currency":"gbp"},"code":"erwkax1md","payee":"User:ABC Paper","transfers":[{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}]},"transfer":{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}}

[0348] --

[0349] BankGateway:MayBank >> sendMoney-reply >> Bank:MayBank

[0350]

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}

[0351] --

[0352] Bank:MayBank >> payInvoice-reply >> User:XYZ Printing

[0353]

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"}

[0354]

[0355] XYZ part-paid invoice {

[0356] "payer": "6wwpwuc",

[0357] "invoice": "erwkax1md",

[0358] "amount": {

[0359] "currency": "GBP",

[0360] "amount": 600

[0361] },

[0362] "id": "ripple-3"

[0363] }

[0364] --

[0365] User:XYZ Printing >> payInvoice >> Bank:MayBank

[0366] {"invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400}}

[0367] --

[0368] Bank:MayBank >> sendMoney >> BankGateway:MayBank

[0369]

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400}}

[0370] --

[0371] BankGateway:MayBank >> getInvoice >> Sparro:Sparro

[0372] "erwkax1md"

[0373] (Sending Payment to Invoice - The payment is sent to the bank that created the invoice.)

[0374] --

[0375] Sparro:Sparro >> getInvoice-reply >> BankGateway:MayBank

[0376] {"bank":"Bank:HSBC"}

[0377] -

[0378] BankGateway:MayBank >> transfer >> BankGateway:HSBC

[0379]

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}

[0380] --

[0381] BankGateway:HSBC >> incomingTransfer >> Bank:HSBC

[0382]

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}

[0383] BankGateway:HSBC >> transfer-reply >> BankGateway:MayBank

[0384] {"success":true,"owed":{"GBP":2000}}

[0385] --

[0386] Bank:HSBC >> incomingTransfer >> User:ABC Paper

[0387]

{"invoice":{"amount":{"amount":2000,"currency":"gbp"},"code":"erwkax1md","payee":"User:ABC Paper","transfers":[{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-3"},{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}]},"transfer":{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}}

[0388] --

[0389] BankGateway:MayBank >> sendMoney-reply >> Bank:MayBank

[0390]

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}

[0391] --

[0392] Bank:MayBank >> payInvoice-reply >> User:XYZ Printing

[0393]

{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"id":"ripple-4"}

[0394] XYZ finished paying invoice {

[0395] "payer": "6wwpwuc",

[0396] "invoice": "erwkax1md",

[0397] "amount": {

[0398] "currency": "GBP",

[0399] "amount": 1400

[0400] },

[0401] "id": "ripple-4"

[0402] }

[0403] features of this embodiment include the enablement of a private, invitation only, network for banking institutions which, in a particular form, can facilitate cross-border payments thereby to enable substantially real-time payments at reduced processing cost.

[0404] With reference to figure 11 there is shown a block diagram of salient characteristics of a messaging system 810 of the prior art as compared with the salient messaging characteristics of the system 1010 enabled by the code listed above and more broadly described with reference to the earlier embodiments.

[0405] Figure 12 illustrates the options for data content to be included in tokens in accordance with embodiments of the invention as described above.

[0406] Figure 13 provides a comparison of characteristics of embodiments of the present invention as compared with the prior art Swift-based messaging system at a commercial layer 1270, a security layer 1271 and a technical layer 1272

[0407] Embodiments of the invention can be implemented utilising the "Ripple" the framework, protocol and gateway-or more generally any blockchain based framework. In a particular form the final settlement process can be enabled through a Ripple frame work thereby to facilitate substantially real-time settlement across multiple institutions and multiple banks.

[0408] Figure 14 is a block diagram of a further embodiment. In this instance a distributed ledger 1381 operating on blockchain principles provides for transmission of the tokenised message as for previous embodiments.

[0409] In this instance it will be observed that the tokenised transmission distributed ledger 1381 operates in parallel with conventional transmission between institution A and institution B.

[0410] Conventional transmission includes transmission of conventional messages utilising the SWIFT protocol. It is also to be noted that institution A and institution B may be subsidiaries of the same institution or may otherwise be closely related. In the alternative they may be completely independent institutions.

[0411] The tokenised message as described in previous embodiments may include information as typically transmitted by the SWIFT or other current acknowledged data transmission systems for transmission of financial information for the purpose of transfer of funds between parties.

[0412] The tokenised message may transmit data which includes some of the data normally included in the conventional message. In alternative forms it may include additional data. In yet alternative forms it may include data not transferred at all in the data normally included in the conventional message.

[0413] The aim, in particular forms, ultimately, is to improve the reliability of the financial transaction as between the first transacting entity and the second transacting entity and, in some forms, to provide an enhanced capability.

[0414] In the arrangement of figure 14 the data comprising the tokenised message is transmitted via nodes 1380 within a blockchain 1381.

[0415] In summary, Bank A and Bank B might be branches of the same bank, say HSBC HK and HSBC China (which today use SWIFT for intrabank transfers). So this system could be used within 1 financial institution.

[0416] In one form the purpose of storing the token only in the blockchain is really to both de-identify the information in the blockchain (which is critical for banks), and enable use of existing (SWIFT / ACH / RTGS) or new messaging systems to send the payment instruction in tokenised format. Banks today have significant investment in existing conventional messaging systems and a complete abandonment of these messaging systems would not be feasible. However settlement is still a manual process so linking the conventional messaging system to the 'blockchain' settlement system (via the token) is an important feature of this embodiment. So, in diagram 7 we include a SWIFT/ACH/RTGS connection between the two Financial Institutions (FIs) (or branches) for communication of the token, and the blockchain ledger is common. The data that is required to settle the payment can be provided by the FI's customer or by the FI themselves (say from a core banking system or similar).

[0417] Fig 15 illustrates in block diagram form key components of an implementation of a blockchain structure which may be utilised to implement the system of figure 14.

[0418] Each block includes verified transactions and the blockchain maintains a ledger all prior transactions. The blockchain is duplicated by all the computers on a network.

[0419] The first block in the chain is known as the Genesis block and new blocks can be added in linear and chronological order. From any given block in the

chain the information of this genesis block and all blocks that led back to this one can be retrieved. A blockchain is essentially numerous blocks connected through hash chaining where each block is comprised of the following (see figure 15);

[0420] Timestamp: provides proof that the data in a block existed at a particular time;

[0421] Previous Hash: Essentially a pointer to the previous block;

[0422] Merkle Hash: Summary of all executed transactions;

[0423] Nonce: Individual blocks identity and is an arbitrary number which can only be used once.

[0424] The blockchain is managed by a network of distributed nodes where each node contains a copy of the entire blockchain. Each node in the network can add blocks to the chain, where every node is adding blocks at the same point in the chain at the same time. The more nodes that comprise the network the harder it is to disrupt the storage of the blockchain. Unlike centralised systems which rely on a single authority, there is no single point of failure in these distributed nodes network. If you change the content of a block you change its Hash.

[0425] Blockchains can be based on/ operate in association with any one of a number of protocols – for example Ripple or Stellar.

[0426] Figure 15B shows a first step in creation of records in the block chain structure of figure 15A whilst figure 15C shows a second step in the creation of records in the chain structure of figure 15A. The chain structures of this type may be utilised in relation to the embodiments described in this application.

[0427] Figure 16 is a block diagram of a further embodiment wherein the parallel data transmission capabilities of the system are further detailed as compared with the embodiment of figure 14 .Components are numbered as for previous embodiments except in the 1400 series. So, for example, first transacting entity 1311 of the further embodiment of figure 14 becomes the first transacting entity 1411. In this instance a distributed ledger 1481 operating on blockchain principles (refer description with reference to figure 15) provides for transmission of the tokenised message as for previous embodiments.

[0428] In this instance it will be observed that the tokenised transmission distributed ledger 1481 operates in parallel with conventional transmission between institution A and institution B.

[0429] Conventional transmission includes transmission of conventional messages utilising the SWIFT protocol. It is also to be noted that institution A 1413 and institution B 1414 may be subsidiaries of the same institution or may otherwise be closely related. In the alternative they may be completely independent institutions.

[0430] The tokenised message 1490 as described in previous embodiments may include information as typically transmitted by the SWIFT or other current acknowledged data transmission systems for transmission of financial information for the purpose of transfer of funds between parties.

[0431] The tokenised message may transmit data which includes some of the data normally included in the conventional message. In alternative forms and more particularly the form with reference to figure 16 it may include additional data however, in this instance the additional data 1491 is transmitted via blockchain 881 as an entry in a shared ledger 1492. The additional data 1491 in this instance comprises a token value 1493, a financial transaction value 1494 a sender cheque status flag 895 and a token state 1496. This entry 1497 in shared ledger 1492 can be accessed based on token value 1493. In an alternative form the entry 1497 and more particularly the token value 1493 may be secured for example requiring a separate key before the data can be accessed and/or decrypted. The data in entry 1497 may comprise deidentified data thereby to ensure that no personally identifiable information is transmitted to Bank (second intermediary entity 1414).

[0432] The aim, ultimately, is to improve the reliability of the financial transaction as between the first transacting entity and the second transacting entity and, in some forms, to provide an enhanced capability.

[0433] In particular, in preferred forms an element includes provision of systems which add additional information whereby the additional information is to enrich payments with more information given the inability of existing payment systems to communicate enriched information.

[0434] In the arrangement of figure 16 the data comprising the tokenised message is transmitted via nodes 1480 within a blockchain 1481.

[0435] In summary, Bank A and Bank B might be branches of the same bank, say HSBC HK and HSBC China (which today use SWIFT for intrabank transfers). So this system could be used within 1 financial institution.

[0436] In one form the purpose of storing the token only in the blockchain is really to both de-identify the information in the blockchain (which is critical for banks), and enable use of existing (SWIFT / ACH / RTGS) or new messaging systems to send the payment instruction in tokenised format. Banks today have significant investment in existing conventional messaging systems and a complete abandonment of these messaging systems would not be feasible. However settlement is still a manual process so linking the conventional messaging system to the 'blockchain' settlement system (via the token) is an important feature of this embodiment. So, in figure 16 we include a SWIFT/ACH/RTGS connection between the two Financial Institutions (FIs) (or branches) for communication of the token, and the blockchain ledger is common. The data that is required to settle the payment can be provided by the FI's customer or by the FI themselves (say from a core banking system or similar).

[0437] Figure 17 is a detailed block diagram of the system of figure 10C and figure 16.

[0438] With reference to Figure 17 there is illustrated in block diagram form a first preferred embodiment of the present invention by way of a non-limiting example of a financial transaction. In this embodiment like components are numbered as for Figure 16 in the 1400 series.

[0439] With reference to figure 17 the financial transaction system 1010 is activated, as for the previous embodiment, when a financial transaction 1020 is entered into between at least first transacting entity 1011 and at least a second transacting entity 1012 each dealing, for the purposes of this transaction, through respective intermediary entities 1013, 1014.

[0440] At the time of and as part of entry into the financial transaction 1020 the first transacting entity 1011 accesses token database 1023 via digital device 1022 executing via a web browser interface or via execution of an application running on a portable digital devices such as a mobile telephone or in a further alternative as a point-of-sale terminal in order to arrange for the database 1023 to generate a token 1021. In this instance the token 1021 will include better data 1024 including the recipient named, BIC, IBAN, destination country, mobile number, currency, business type, communication, payment amount. In this instance the token 1021 including the metadata 1024 is stored in the token database 1023. In addition the first transacting entity 1011 communicates the token 1021 to a digital device 1030 associated with second transacting entity 1012. In this instance the communication is by way of initial transmission of the token 1021 to digital device 1022 which then on transmits the token via Internet 1031 to digital device 1030.

[0441] With reference to figure 17, when ready to settle the financial transaction 1020 the second transacting entity 1012 "logs in" to a portal associated with second intermediary entity 1014 and communicates the token 1021. In this instance have the login can be executed via a web browser associated with digital device 1030 which communicates via Internet 1031 the token 1021 to a digital processing system 1032 (including at least a processor and a memory) associated with second intermediary entity 1014. Substantially at the same time as part of seeking to settle the financial transaction 1020:

[0442] Notification: token database 1023 notifies second intermediary entity 1014 to contact the token database 1023 from which it receives a further token 1021A.

[0443] Verification: token database 1023 communicates with the processing system 1032 of second intermediary entity 1014 to verify that sufficient funds are located

in account 1016 as indicated in the meta data 1024 to settle the financial transaction.

[0444] Committing payer funds: payers bank debits payers account: payers bank sends notice to payer bank gateway: payers bank gateway calls token database 1023 to get approved token:

[0445] Settlement: gateway of payers bank sends by way of non-limiting example XRP (the native currency of the Ripple protocol) to billers bank gateway: payers bank gateway notifies token database 1023 of receipt:

[0446] Clearing: payer's bank may be a Nostro account which is debited subject to bank institution rules.

[0447] Embodiments of the invention can be implemented utilising the "Ripple" framework, protocol and gateway-or more generally any blockchain based framework. In a particular form the final settlement process can be enabled through a Ripple framework thereby to facilitate substantially real-time settlement across multiple institutions and multiple banks.

[0448] With further reference to figure 17 it will be observed that the token 1021, in this instance, may be conveyed between bank 1013 and bank 1014 by way of a medium 1060 utilizing the SWIFT protocol or other compatible protocols 1050. In preferred forms the medium the medium will be an electronic communications medium and in particular forms may be implemented by way of a VPN established between bank 1013 and bank 1014.

[0449] Separately deidentified data 1051 A, B, C, D associated with the financial transaction to which the token pertains may be transmitted over a separate communication medium, in this instance internet 1031. In a preferred form the communication medium utilizes a blockchain structure as described earlier in this specification and the deidentified data 1051 A, B, C, D is located within a record structure 1061 which is replicated throughout the blockchain structure.

[0450] In use a sellers bank 1013 as part of entering into the financial transaction with buyers bank 1014 will establish a SWIFT transaction transmittable over medium 1060. Separately and preferably in parallel the sellers bank 1013 will perform associated operations needed to complete the financial transaction such as verification of the buyers ID and related characteristics. Data related to these associated operations is then placed in record structure 1061 and that record is placed into the blockchain structure. The associated data includes deidentifed data 1051 A, B, C, D.

[0451] This data is available to the buyers bank 1014 by way of the buyers bank logging into the blockchain structure and receiving the deidentified data which is associated with the financial transaction which is represented by token 1021. Thereby allowing assembly by the buyers bank 1014 of all necessary data to execute the financial transaction on behalf of the buyer and seller.

[0452] With reference to figures 16 and 17 the system provides for communication of invoice/purchase order /remittance advice information as illustrated.

[0453] It will be further observed that blockchain structures may be utilized to provide an information layer above existing legacy systems (for example based on SWIFT protocols and the like) and wherein the additional information layer provides enriched information about payments using the token. It is to be noted that existing systems do not provide enriched information and, in more particular forms, do not provide deidentified information/data for use by the communicating parties.

[0454] The above describes only some embodiments of the present invention and modifications, obvious to those skilled in the art, can be made thereto without departing from the scope of the present invention.

[0455] The computer implemented method and the system for processing a financial transaction offers a plurality of advantages. First, the invention enables a wide variety of documents to be attached to a financial transaction, by means of a token. The existing financial messaging systems allow only specific information to be attached to the financial transaction. Further, the invention enables

generation of an auditable enriched data record from the documents. The enriched data record is stored in a distributed ledger (or the blockchain) and can be retrieved at any time when queried with the token. Further, the enriched data record ensures that integrity of the documents is maintained in perpetuity. Further, the documents stores enable maintaining of a state of the token. That is, a status of the financial transaction can be tracked at any time, from the respective documents stored in the document stores.

Other Exemplary Embodiments

[0456] Definitions:

[0457] Token: in this specification a "token" is a pointer to an enriched data record of a plurality data required to process a financial transaction and wherein the plurality of data is rendered, formatted or passed through an algorithm in a predetermined manner. The process of rendering, formatting or passing through an algorithm in a predetermined manner is termed “tokenisation”. The tokenisation process may involve operations such as encryption and de-identification of the plurality of data.

[0458] Financial Transaction: in this specification "financial transaction" refers to a trade between two parties, for example at least a first transacting entity and a second transacting entity and wherein the trade is expressed in a financial form (for example in a Fiat currency or an electronic currency-to be distinguished, for example, from a barter transaction) which will ultimately require exchange of currency to process the financial transaction. In some instances the currency will be the same on both sides of the financial transaction. In other cases a conversion from one currency to another may be required.

[0459] Personally Identifiable Information (PII): in this specification refers to information that a regulator or privacy policy will not allow to be disclosed to a third party.

[0460] Accordingly, in one broad form of the invention, there is provided a system for settling a financial transaction electronically; said system comprising:

at least a first transacting entity;

at least a second transacting entity;

at least a first intermediary entity;

at least a second intermediary entity;

in the case where the first transacting entity enters into a financial transaction with the second transacting entity generating a tokenised message at the time of the financial transaction containing data needed to settle the financial transaction;

initiating settlement of the financial transaction by transmission of the tokenised message to the at least first transacting entity.

[0461] In a further broad form of the invention there is provided a tokenised message construction system; said system comprising:

a server in communication with a database and which facilitates communications between a plurality of parties to a financial transaction;

each party having a digitised device with which to communicate with other ones of the parties and with the server;

each party capable of generating a tokenised message via a bidirectional communication with the server.

[0462] Accordingly, in yet a further broad form of the invention there is provided tokenised message construction system; said system comprising:

a server in communication with a database and which facilitates communications between a plurality of parties to a financial transaction;

each party having a digitised device with which to communicate with other ones the parties and with the server;

each party capable of generating a tokenised message via a bidirectional communication with the server.

[0463] Preferably the tokenised message is generated with reference to a token database located at a remote location.

[0464] Preferably the tokenised message includes at least a first data element, a second data element and a third data element.

[0465] Preferably the first data element comprises identification data for a payor, the second data element comprises identification data for a payee (biller) and the third data element comprises identification currency, denomination and value data.

[0466] Preferably a further tokenised message is generated by either an intermediary entity or the token database.

[0467] Preferably a tokenised message is generated by a bi-directional communication process.

[0468] Preferably the bi-directional communication process is between the token database and an intermediary entity.

[0469] Preferably a step in producing a tokenised message involves de-identifying data.

[0470] Preferably a step in producing a tokenised message involves adding a data element to the message.

[0471] Preferably a step in producing a tokenised message involves removing a data element from the message.

[0472] Preferably a step in producing a tokenised message involves applying an algorithm to the data elements in the message.

[0473] Preferably the token database sequences the tokenised messages.

[0474] Preferably the token database sequences the tokenised messages and transmits the tokenised messages as payment data records to a blockchain settlement system.

[0475] Preferably the blockchain settlement system employs the Ripple protocol.

[0476] Preferably the tokenised message includes at least a first data element, a second data element and a third data element.

[0477] Preferably the first data element comprises identification data for a payor, the second data element comprises identification data for a payee (biller) and the third data element comprises identification currency, denomination and value data.

[0478] Preferably a further tokenised message is generated by either an intermediary entity or the token database.

[0479] Preferably a tokenised message is generated by a bi-directional communication process.

[0480] Preferably the bi-directional communication process is between the token database and an intermediary entity.

[0481] Preferably a step in producing a tokenised message involves de-identifying data.

[0482] Preferably a step in producing a tokenised message involves adding a data element to the message.

[0483] Preferably a step in producing a tokenised message involves removing a data element from the message.

[0484] Preferably a step in producing a tokenised message involves applying an algorithm to the data elements in the message.

[0485] Preferably the token database sequences the tokenised messages.

[0486] Preferably the token database sequences the tokenised messages and transmits the tokenised messages as payment data records to a blockchain settlement system.

[0487] Preferably the blockchain settlement system employs the Ripple protocol.

[0488] Preferably a second message is transmitted between the intermediaries.

[0489] Preferably the second message is tokenised.

[0490] Preferably the second message contains conventional data.

[0491] Preferably the second message is transmitted by means of a blockchain system.

[0492] Preferably the second message includes information equivalent to that transmitted by the SWIFT system.

[0493] Preferably the tokenised message includes additional information beyond that transmitted by the SWIFT system.

[0494] The system wherein the tokenised message includes information which verifies the security status of at least one party to the financial transaction.

[0495] Preferably the second tokenised message includes information which verifies the security status of both parties to the financial transaction.

[0496] Preferably the token is conveyed by way of a medium utilizing the SWIFT messaging system or other compatible messaging system.

[0497] Preferably the medium is implemented by way of a VPN.

[0498] Preferably deidentified data associated with the financial transaction to which the token pertains is transmitted over a separate communication medium.

[0499] Preferably the separate communication medium utilizes a blockchain structure.

[0500] Preferably the deidentified data is located within a record structure which is replicated throughout the blockchain structure.

[0501] Preferably in use a sellers bank as part of entering into the financial transaction with buyers bank will establish a SWIFT transaction.

[0502] Preferably in parallel the sellers bank will perform associated operations needed to complete the financial transaction such as verification of the buyers ID and related characteristics.

[0503] Preferably data related to the associated operations is then placed in a record structure and that record is placed into the blockchain structure.

[0504] Preferably the associated data includes deidentifed data.

[0505] Preferably the data is available to the buyers bank by way of the buyers bank logging into the blockchain structure and receiving the deidentified data which is associated with the financial transaction which is represented by the token thereby allowing assembly by the buyers bank of all necessary data to execute the financial transaction on behalf of the buyer and seller.

[0506] Preferably incorporating secure channels thereby permitting only selected entities to communicate the data to execute the financial transaction on behalf of the buyer and seller.

Advantages

[0507] The invention is not limited to interaction between two banks only, but can be extended to any number of banks involved in the financial transaction. For example, the token can be included in all the financial messages sent between a plurality of banks, and the token can be used by any bank from the plurality of banks to verify the financial transaction from the enriched data record, before taking any further steps in the process.

[0508] The messaging bus allows all the financial institutions involved in the financial transaction to communicate in real-time and ensure that the payer, the

beneficiary, and all the parameters corresponding to the financial transaction are validated. Further, encryption/decryption of the requests and responses using asymmetrical pairs of keys ensures that the transmission of the request and the responses is always secure. Further, the payment risk rating ensures better straight through processing by reducing exceptions and false positives. Also, the token is compatible with a large array of formats, including JSON, XML, CSV, SWIFT, over a number of transports, including HTTP, FTP, AMQP, and JMS.

Interpretation

[0509] Unless otherwise defined, all terms (including technical and scientific terms) used herein have the same meaning as commonly understood by one of ordinary skill in the art to which this invention belongs. It will be further understood that terms used herein should be interpreted as having a meaning that is consistent with their meaning in the context of this specification and the relevant art and will not be interpreted in an idealized or overly formal sense unless expressly so defined herein. For the purposes of the present invention, additional terms are defined below. Furthermore, all definitions, as defined and used herein, should be understood to control over dictionary definitions, definitions in documents incorporated by reference, and/or ordinary meanings of the defined terms unless there is doubt as to the meaning of a particular term, in which case the common dictionary definition and/or common usage of the term will prevail.

[0510] The terminology used herein is for the purpose of describing particular embodiments only and is not intended to be limiting of the invention. As used herein, the singular articles “a”, “an” and “the” are intended to include the plural forms as well, unless the context clearly indicates otherwise and thus are used herein to refer to one or to more than one (i.e. to “at least one”) of the grammatical object of the article. By way of example, the phrase “an element” refers to one element or more than one element.

[0511] The term “about” is used herein to refer to quantities that vary by as much as 30%, preferably by as much as 20%, and more preferably by as much as 10% to a reference quantity. The use of the word ‘about’ to qualify a number is merely an express indication that the number is not to be construed as a precise value.

[0512] Throughout this specification, unless the context requires otherwise, the words "comprise", "comprises" and "comprising" will be understood to imply the inclusion of a stated step or element or group of steps or elements but not the exclusion of any other step or element or group of steps or elements.

[0513] The term "real-time" for example "displaying real-time data," refers to the display of the data without intentional delay, given the processing limitations of the system and the time required to accurately measure the data.

[0514] As used herein, the term "exemplary" is used in the sense of providing examples, as opposed to indicating quality. That is, an "exemplary embodiment" is an embodiment provided as an example, as opposed to necessarily being an embodiment of exemplary quality for example serving as a desirable model or representing the best of its kind.

[0515] The phrase "and/or," as used herein in the specification and in the claims, should be understood to mean "either or both" of the elements so conjoined, i.e., elements that are conjunctively present in some cases and disjunctively present in other cases. Multiple elements listed with "and/or" should be construed in the same fashion, i.e., "one or more" of the elements so conjoined. Other elements may optionally be present other than the elements specifically identified by the "and/or" clause, whether related or unrelated to those elements specifically identified. Thus, as a non-limiting example, a reference to "A and/or B", when used in conjunction with open-ended language such as "comprising" can refer, In one embodiment of the invention, to A only (optionally including elements other than B); in another embodiment, to B only (optionally including elements other than A); in yet another embodiment, to both A and B (optionally including other elements); etc.

[0516] As used herein in the specification and in the claims, "or" should be understood to have the same meaning as "and/or" as defined above. For example, when separating items in a list, "or" or "and/or" shall be interpreted as being inclusive, i.e., the inclusion of at least one, but also including more than one, of a number or list of elements, and, optionally, additional unlisted items. Only terms clearly indicated to the contrary, such as "only one of" or "exactly one

of," or, when used in the claims, "consisting of" will refer to the inclusion of exactly one element of a number or list of elements. In general, the term "or" as used herein shall only be interpreted as indicating exclusive alternatives (i.e. "one or the other but not both") when preceded by terms of exclusivity, such as "either," "one of," "only one of," or "exactly one of." "Consisting essentially of," when used in the claims, shall have its ordinary meaning as used in the field of patent law.

[0517] As used herein in the specification and in the claims, the phrase "at least one," in reference to a list of one or more elements, should be understood to mean at least one element selected from any one or more of the elements in the list of elements, but not necessarily including at least one of each and every element specifically listed within the list of elements and not excluding any combinations of elements in the list of elements. This definition also allows that elements may optionally be present other than the elements specifically identified within the list of elements to which the phrase "at least one" refers, whether related or unrelated to those elements specifically identified. Thus, as a non-limiting example, "at least one of A and B" (or, equivalently, "at least one of A or B," or, equivalently "at least one of A and/or B") can refer, In one embodiment of the invention, to at least one, optionally including more than one, A, with no B present (and optionally including elements other than B); in another embodiment, to at least one, optionally including more than one, B, with no A present (and optionally including elements other than A); in yet another embodiment, to at least one, optionally including more than one, A, and at least one, optionally including more than one, B (and optionally including other elements); etc.

Bus

[0518] In the context of this document, the term "bus" and its derivatives, while being described in a preferred embodiment as being a communication bus subsystem for interconnecting various devices including by way of parallel connectivity such as Industry Standard Architecture (ISA), conventional Peripheral Component Interconnect (PCI) and the like or serial connectivity such as PCI Express (PCIe), Serial Advanced Technology Attachment (Serial ATA) and the like, should be construed broadly herein as any system for communicating data.

In accordance with:

[0519] As described herein, 'in accordance with' may also mean 'as a function of' and is not necessarily limited to the integers specified in relation thereto.

Composite items

[0520] As described herein, 'a computer implemented method' should not necessarily be inferred as being performed by a single computing device such that the steps of the computer implemented method may be performed by more than one cooperating computing devices.

[0521] Similarly objects as used herein such as 'web server', 'server', 'client computing device', 'computer readable medium' and the like should not necessarily be construed as being a single object, and may be implemented as a two or more objects in cooperation, such as, for example, a web server being construed as two or more web servers in a server farm cooperating to achieve a desired goal or a computer readable medium being distributed in a composite manner, such as program code being provided on a compact disk activatable by a license key downloadable from a computer network.

Database:

[0522] In the context of this document, the term "database" and its derivatives may be used to describe a single database, a set of databases, a system of databases or the like. The system of databases may comprise a set of databases wherein the set of databases may be stored on a single implementation or span across multiple implementations. The term "database" is also not limited to refer to a certain database format rather may refer to any database format. For example, database formats may include MySQL, MySQLi , XML or the like.

Wireless:

[0523] The invention may be embodied using devices conforming to other network standards and for other applications, including, for example other WLAN standards and other wireless standards. Applications that can be accommodated include IEEE 802.11 wireless LANs and links, and wireless Ethernet.

[0524] In the context of this document, the term "wireless" and its derivatives may be used to describe circuits, devices, systems, methods, techniques, communications channels, etc., that may communicate data through the use of modulated electromagnetic radiation through a non-solid medium. The term does not imply that the associated devices do not contain any wires, although in some embodiments they might not. In the context of this document, the term "wired" and its derivatives may be used to describe circuits, devices, systems, methods, techniques, communications channels, etc., that may communicate data through the use of modulated electromagnetic radiation through a solid medium. The term does not imply that the associated devices are coupled by electrically conductive wires.

Processes:

[0525] Unless specifically stated otherwise, as apparent from the following discussions, it is appreciated that throughout the specification discussions utilizing terms such as "processing", "computing", "calculating", "determining", "analysing" or the like, refer to the action and/or processes of a computer or computing system, or similar electronic computing device, that manipulate and/or transform data represented as physical, such as electronic, quantities into other data similarly represented as physical quantities.

Processor:

[0526] In a similar manner, the term "processor" may refer to any device or portion of a device that processes electronic data, e.g., from registers and/or memory to transform that electronic data into other electronic data that, e.g., may be stored in registers and/or memory. A "computer" or a "computing device" or a "computing machine" or a "computing platform" may include one or more processors.

[0527] The computer implemented methodologies described herein are, In one embodiment of the invention, performable by one or more processors that accept computer-readable (also called machine-readable) code containing a set of instructions that when executed by one or more of the processors carry out at least one of the computer implemented methods described herein. Any processor capable of executing a set of instructions (sequential or otherwise) that specify actions to be taken are included. Thus, one example is a typical

processing system that includes one or more processors. The processing system further may include a memory subsystem including main RAM and/or a static RAM, and/or ROM.

Computer-Readable Medium:

[0528] Furthermore, a computer-readable carrier medium may form, or be included in a computer program product. A computer program product can be stored on a computer usable carrier medium, the computer program product comprising a computer readable program means for causing a processor to perform a method as described herein.

Networked or Multiple Processors:

[0529] In alternative embodiments, the one or more processors operate as a standalone device or may be connected, e.g., networked to other processor(s), in a networked deployment, the one or more processors may operate in the capacity of a server or a client machine in server-client network environment, or as a peer machine in a peer-to-peer or distributed network environment. The one or more processors may form a web appliance, a network router, switch or bridge, or any machine capable of executing a set of instructions (sequential or otherwise) that specify actions to be taken by that machine.

[0530] Note that while some diagram(s) only show(s) a single processor and a single memory that carries the computer-readable code, those in the art will understand that many of the components described above are included, but not explicitly shown or described in order not to obscure the inventive aspect. For example, while only a single machine is illustrated, the term "machine" shall also be taken to include any collection of machines that individually or jointly execute a set (or multiple sets) of instructions to perform any one or more of the computer implemented methodologies discussed herein.

Additional Embodiments:

[0531] Thus, one embodiment of each of the computer implemented methods described herein is in the form of a computer-readable carrier medium carrying a set of instructions, e.g., a computer program that are for execution on one or more processors. Thus, as will be appreciated by those skilled in the art, embodiments of the present invention may be embodied as a method, an

apparatus such as a special purpose apparatus, an apparatus such as a data processing system, or a computer-readable carrier medium. The computer-readable carrier medium carries computer readable code including a set of instructions that when executed on one or more processors cause a processor or processors to implement a method. Accordingly, aspects of the present invention may take the form of a method, an entirely hardware embodiment, an entirely software embodiment or an embodiment combining software and hardware aspects. Furthermore, the present invention may take the form of carrier medium (e.g., a computer program product on a computer-readable storage medium) carrying computer-readable program code embodied in the medium.

Carrier Medium:

[0532] The software may further be transmitted or received over a network via a network interface device. While the carrier medium is shown in an example embodiment to be a single medium, the term "carrier medium" should be taken to include a single medium or multiple media (e.g., a centralized or distributed database, and/or associated caches and servers) that store the one or more sets of instructions. The term "carrier medium" shall also be taken to include any medium that is capable of storing, encoding or carrying a set of instructions for execution by one or more of the processors and that cause the one or more processors to perform any one or more of the computer implemented methodologies of the present invention. A carrier medium may take many forms, including but not limited to, non-volatile media, volatile media, and transmission media.

Implementation:

[0533] It will be understood that the steps of methods discussed are performed In one embodiment of the invention by an appropriate processor (or processors) of a processing (i.e., computer) system executing instructions (computer-readable code) stored in storage. It will also be understood that the invention is not limited to any particular implementation or programming technique and that the invention may be implemented using any appropriate techniques for implementing the functionality described herein. The invention is not limited to any particular programming language or operating system.

Means For Carrying out a Method or Function

[0534] Furthermore, some of the embodiments are described herein as a method or combination of elements of a method that can be implemented by a processor of a processor device, computer system, or by other means of carrying out the function. Thus, a processor with the necessary instructions for carrying out such a method or element of a method forms a means for carrying out the computer implemented method or element of a method. Furthermore, an element described herein of an apparatus embodiment is an example of a means for carrying out the function performed by the element for the purpose of carrying out the invention.

Connected

[0535] Similarly, it is to be noticed that the term connected, when used in the claims, should not be interpreted as being limitative to direct connections only. Thus, the scope of the expression a device A connected to a device B should not be limited to devices or systems wherein an output of device A is directly connected to an input of device B. It means that there exists a path between an output of A and an input of B which may be a path including other devices or means. "Connected" may mean that two or more elements are either in direct physical or electrical contact, or that two or more elements are not in direct contact with each other but yet still co-operate or interact with each other.

Embodiments:

[0536] Reference throughout this specification to "one embodiment" or "an embodiment" means that a particular feature, structure or characteristic described in connection with the embodiment is included in at least one embodiment of the present invention. Thus, appearances of the phrases "In one embodiment of the invention" or "in an embodiment" in various places throughout this specification are not necessarily all referring to the same embodiment, but may. Furthermore, the particular features, structures or characteristics may be combined in any suitable manner, as would be apparent to one of ordinary skill in the art from this disclosure, in one or more embodiments.

[0537] Similarly it should be appreciated that in the above description of example embodiments of the invention, various features of the invention are sometimes grouped together in a single embodiment, figure, or description thereof for the

purpose of streamlining the disclosure and aiding in the understanding of one or more of the various inventive aspects. This method of disclosure, however, is not to be interpreted as reflecting an intention that the claimed invention requires more features than are expressly recited in each claim. Rather, as the following claims reflect, inventive aspects lie in less than all features of a single foregoing disclosed embodiment. Thus, the claims following the Detailed Description of Specific Embodiments are hereby expressly incorporated into this Detailed Description of Specific Embodiments, with each claim standing on its own as a separate embodiment of this invention.

[0538] Furthermore, while some embodiments described herein include some but not other features included in other embodiments, combinations of features of different embodiments are meant to be within the scope of the invention, and form different embodiments, as would be understood by those in the art. For example, in the following claims, any of the claimed embodiments can be used in any combination.

Specific Details

[0539] In the description provided herein, numerous specific details are set forth. However, it is understood that embodiments of the invention may be practiced without these specific details. In other instances, well-known methods, structures and techniques have not been shown in detail in order not to obscure an understanding of this description.

[0540] It will be appreciated that the computer implemented methods and systems described/illustrated above at least substantially provides a manner in which data generated in an EHR, during an episode of care, may be de-identified (or anonymized) and provided to a user through a secure channel.

[0541] The embodiments described herein, and/or shown in the drawings, are presented by way of example only and are not limiting as to the scope of the invention. Unless otherwise specifically stated, individual aspects and components of the embodiments may be modified, or may have been substituted therefore known equivalents, or as yet unknown substitutes such as may be developed in the future or such as may be found to be acceptable substitutes in

the future. The embodiments may also be modified for a variety of applications while remaining within the scope and spirit of the claimed invention, since the range of potential applications is great, and since it is intended that the present invention be adaptable to many such variations.

Different Instances of Objects

[0542] As used herein, unless otherwise specified the use of the ordinal adjectives "first", "second", "third", etc., to describe a common object, merely indicate that different instances of like objects are being referred to, and are not intended to imply that the objects so described must be in a given sequence, either temporally, spatially, in ranking, or in any other manner.

Comprising and Including

[0543] In the claims which follow and in the preceding description of the invention, except where the context requires otherwise due to express language or necessary implication, the word "comprise" or variations such as "comprises" or "comprising" are used in an inclusive sense, i.e. to specify the presence of the stated features but not to preclude the presence or addition of further features in various embodiments of the invention.

[0544] Any one of the terms: including or which includes or that includes as used herein is also an open term that also means including at least the elements/features that follow the term, but not excluding others. Thus, including is synonymous with and means comprising.

Scope of Invention

[0545] Thus, while there has been described what are believed to be the preferred embodiments of the invention, those skilled in the art will recognize that other and further modifications may be made thereto without departing from the spirit of the invention, and it is intended to claim all such changes and modifications as fall within the scope of the invention. For example, any formulas given above are merely representative of procedures that may be used. Functionality may be added or deleted from the block diagrams and operations may be interchanged among functional blocks. Steps may be added or deleted to methods described within the scope of the present invention.

[0546] Although the invention has been described with reference to specific examples, it will be appreciated by those skilled in the art that the invention may be embodied in many other forms.

Chronological order

[0547] For the purpose of this specification, where method steps are described in sequence, the sequence does not necessarily mean that the steps are to be carried out in chronological order in that sequence, unless there is no other logical manner of interpreting the sequence.

Industrial Applicability

[0548] It is apparent from the above, that the arrangements described are applicable to the industries dealing with banking, brokerages, insurance companies, investment companies and Unit Investment Trusts (UIT) etc.

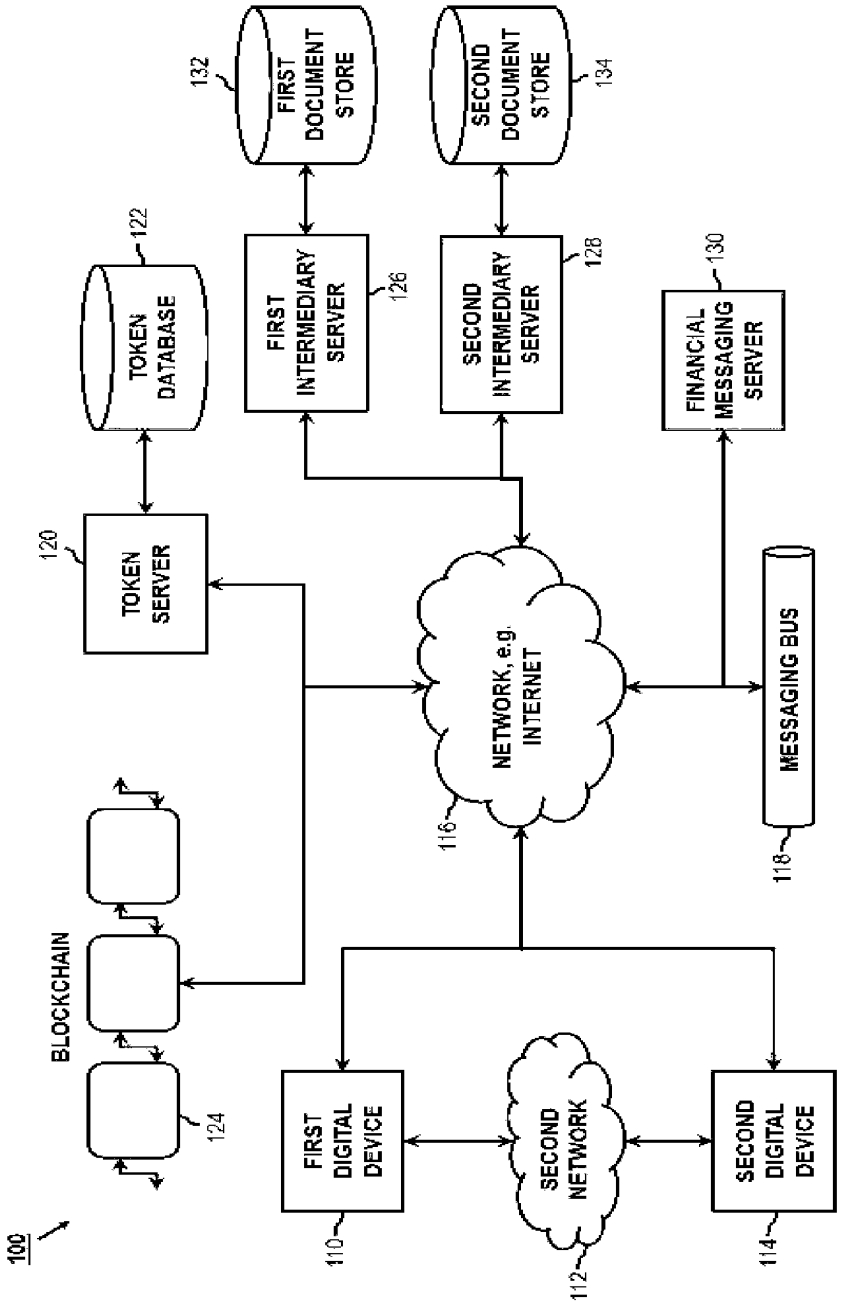

100
FIRST DIGITAL DEVICE
110
SECOND NETWORK
112
SECOND DIGITAL DEVICE
114
BLOCKCHAIN
124
NETWORK, e.g. INTERNET
116
MESSAGING BUS
118
TOKEN SERVER
120
TOKEN DATABASE
122
FIRST INTERMEDIARY SERVER
126
SECOND INTERMEDIARY SERVER
128
FINANCIAL MESSAGING SERVER
130
FIRST DOCUMENT STORE
132
SECOND DOCUMENT STORE
134

FIG. 1

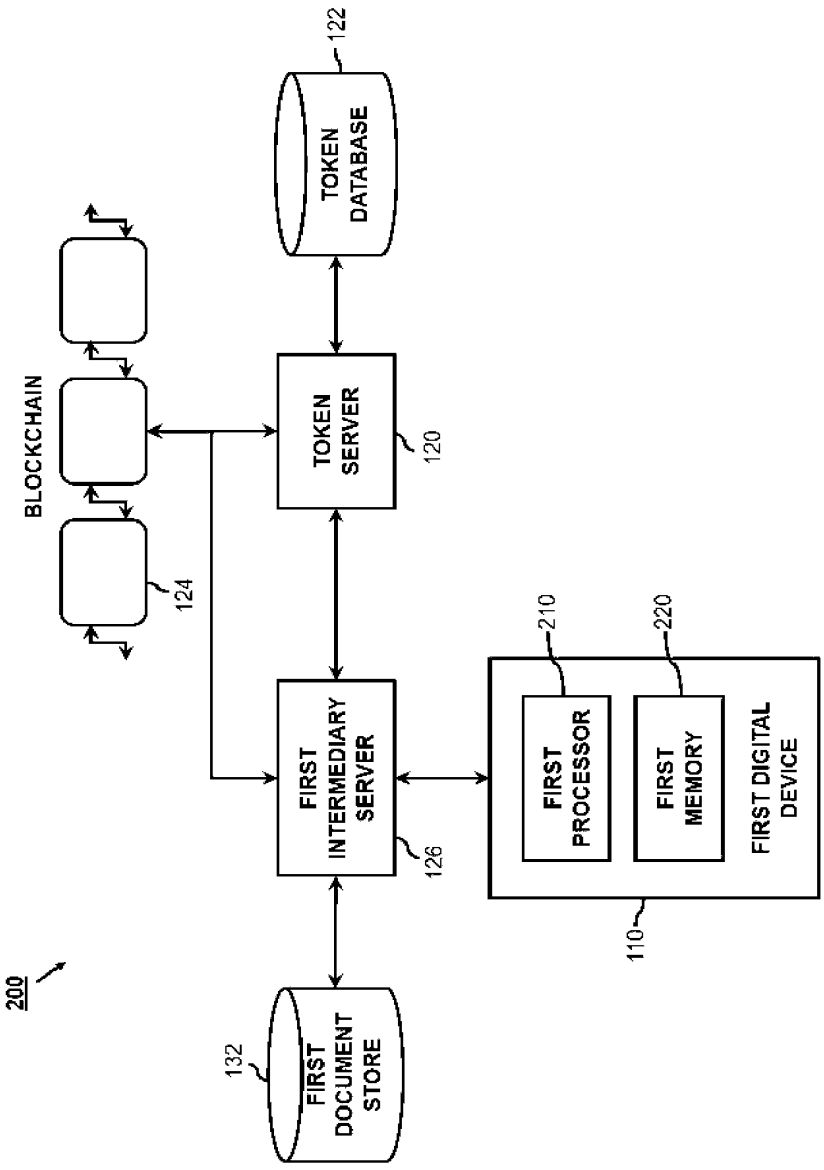

200
TOKEN DATABASE
122
BLOCKCHAIN
124
TOKEN SERVER
120
FIRST INTERMEDIARY SERVER
126
FIRST DOCUMENT STORE
132
210
220
FIRST PROCESSOR
FIRST MEMORY
FIRST DIGITAL DEVICE
110

FIG. 2

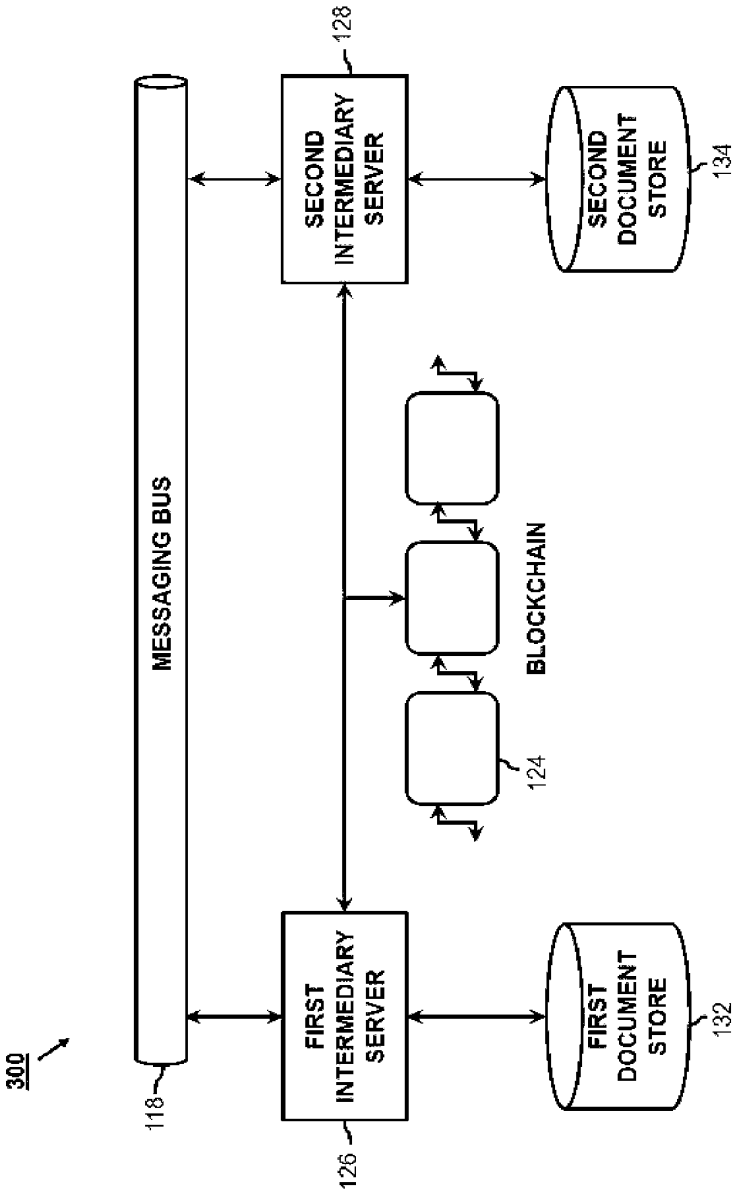

300
MESSAGING BUS
118
FIRST INTERMEDIARY SERVER
126
FIRST DOCUMENT STORE
132
SECOND INTERMEDIARY SERVER
128
SECOND DOCUMENT STORE
134
BLOCKCHAIN
124

FIG. 3

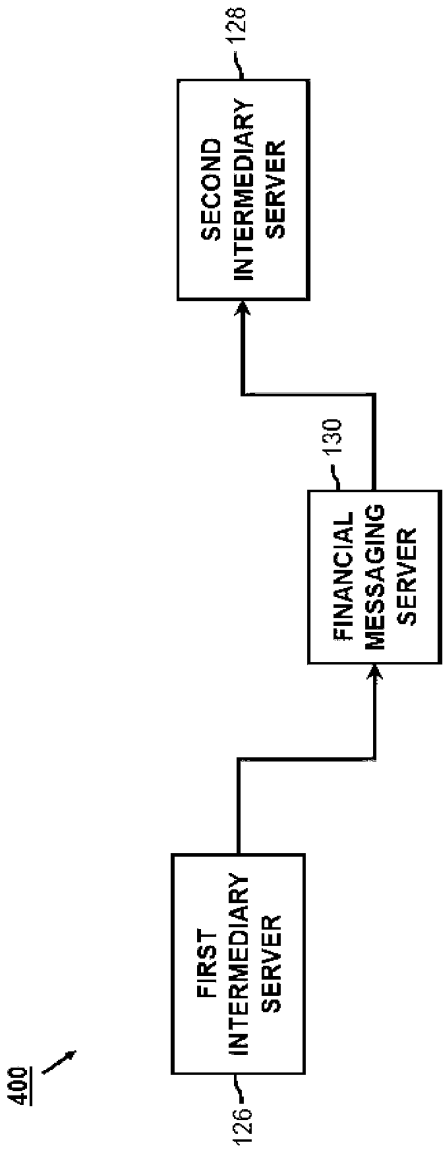

400
FIRST INTERMEDIARY SERVER
126
FINANCIAL MESSAGING SERVER
130
SECOND INTERMEDIARY SERVER
128

FIG. 4

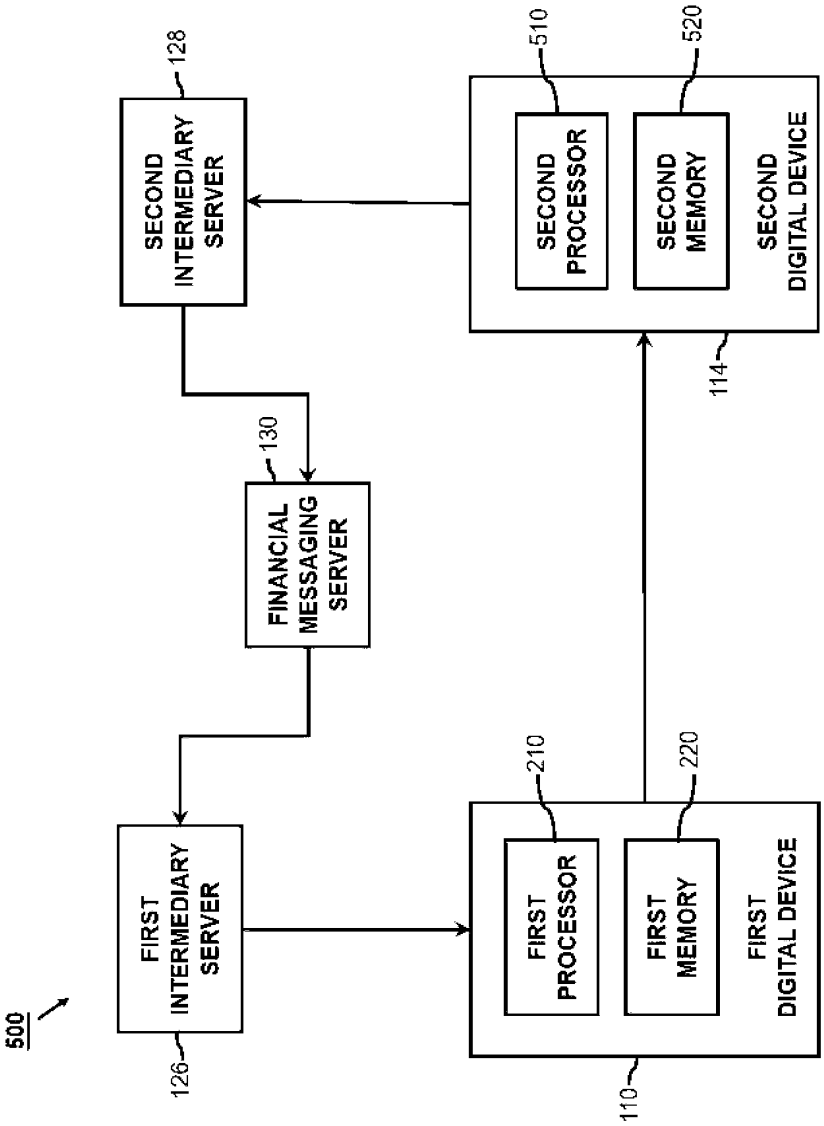

500
FIRST INTERMEDIARY SERVER
126
FINANCIAL MESSAGING SERVER
130
SECOND INTERMEDIARY SERVER
128
FIRST PROCESSOR
210
FIRST MEMORY
220
FIRST DIGITAL DEVICE
110
SECOND PROCESSOR
510
SECOND MEMORY
520
SECOND DIGITAL DEVICE
114

FIG. 5

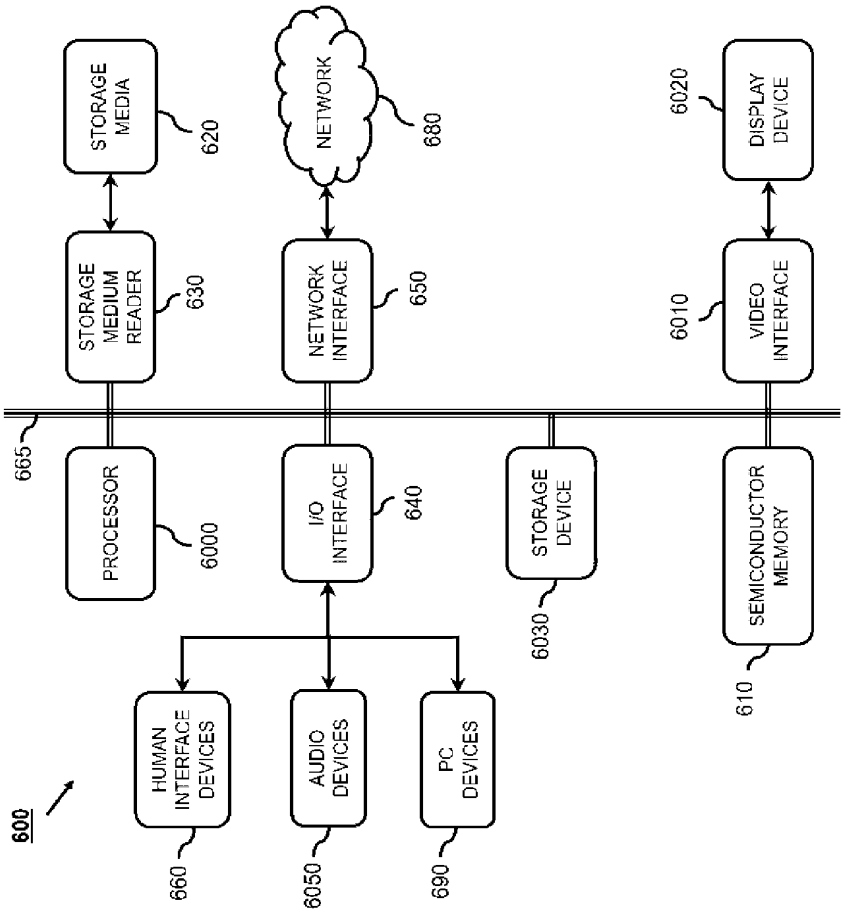

600
665
PROCESSOR
6000
STORAGE MEDIUM READER
630
STORAGE MEDIA
620
I/O INTERFACE
640
NETWORK INTERFACE
650
NETWORK
680
STORAGE DEVICE
6030
VIDEO INTERFACE
6010
DISPLAY DEVICE
6020
SEMICONDUCTOR MEMORY
610
HUMAN INTERFACE DEVICES
660
AUDIO DEVICES
6050
PC DEVICES
690

FIG. 6

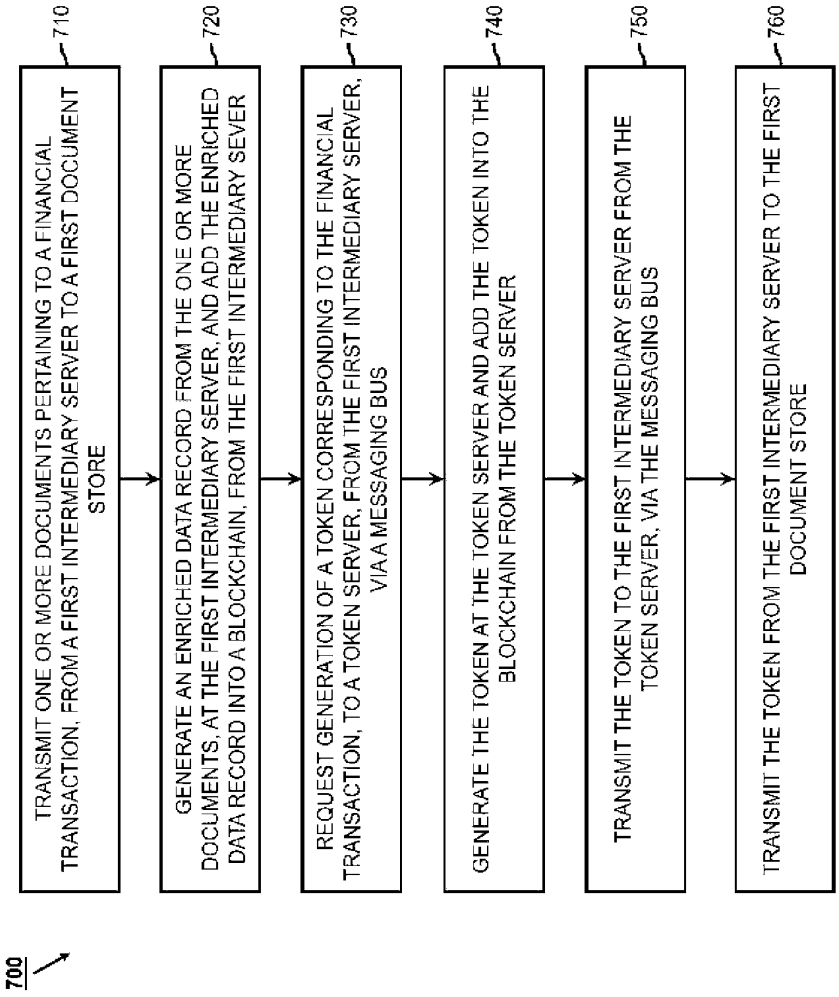

700
710
TRANSMIT ONE OR MORE DOCUMENTS PERTAINING TO A FINANCIAL TRANSACTION, FROM A FIRST INTERMEDIARY SERVER TO A FIRST DOCUMENT STORE
720
GENERATE AN ENRICHED DATA RECORD FROM THE ONE OR MORE DOCUMENTS, AT THE FIRST INTERMEDIARY SERVER, AND ADD THE ENRICHED DATA RECORD INTO A BLOCKCHAIN, FROM THE FIRST INTERMEDIARY SEVER
730
REQUEST GENERATION OF A TOKEN CORRESPONDING TO THE FINANCIAL TRANSACTION, TO A TOKEN SERVER, FROM THE FIRST INTERMEDIARY SERVER, VIA A MESSAGING BUS
740
GENERATE THE TOKEN AT THE TOKEN SERVER AND ADD THE TOKEN INTO THE BLOCKCHAIN FROM THE TOKEN SERVER
750
TRANSMIT THE TOKEN TO THE FIRST INTERMEDIARY SERVER FROM THE TOKEN SERVER, VIA THE MESSAGING BUS
760
TRANSMIT THE TOKEN FROM THE FIRST INTERMEDIARY SERVER TO THE FIRST DOCUMENT STORE

FIG. 7

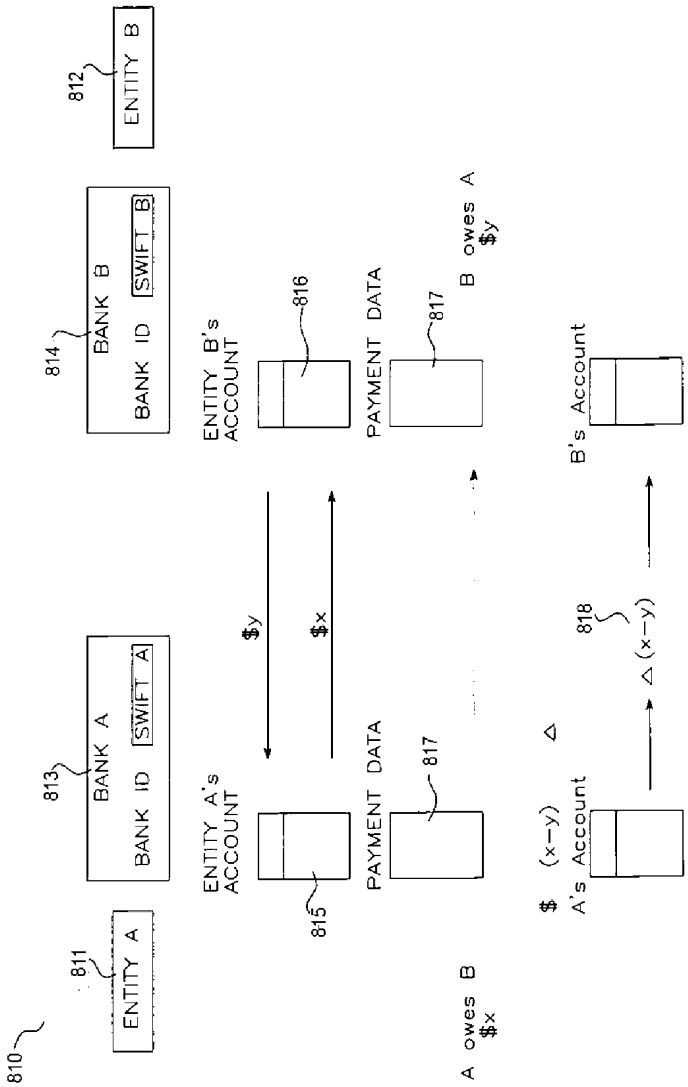


FIG. 8A
[PRIOR ART]

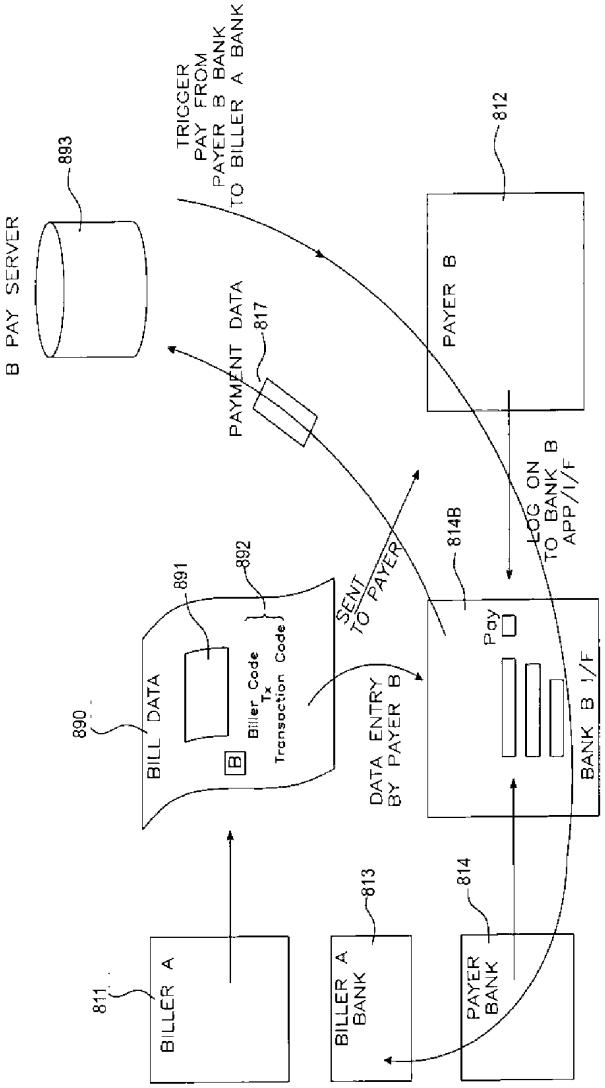


FIG. 8B
[PRIOR ART]

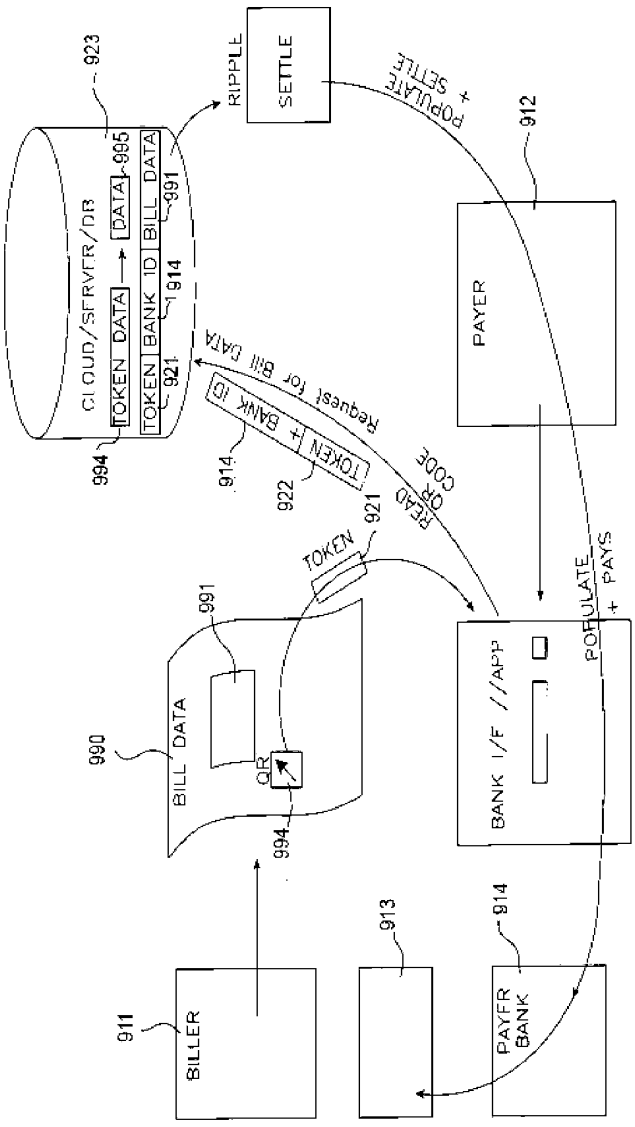

923
CLOUD/SERVER/DB
TOKEN DATA
BANK ID
DATA
BILL DATA
995
991
914
921
994
RIPPLE
SETTLE
POPULATE + SETTLE
912
PAYER
Request for Bill DATA
TOKEN + BANK ID
914
922
921
READ QR CODE
TOKEN
991
990
BILL DATA
QR
994
BANK I/F //APP
POPULATE + PAYS
911
BILLER
913
914
PAYER BANK

FIG. 9A

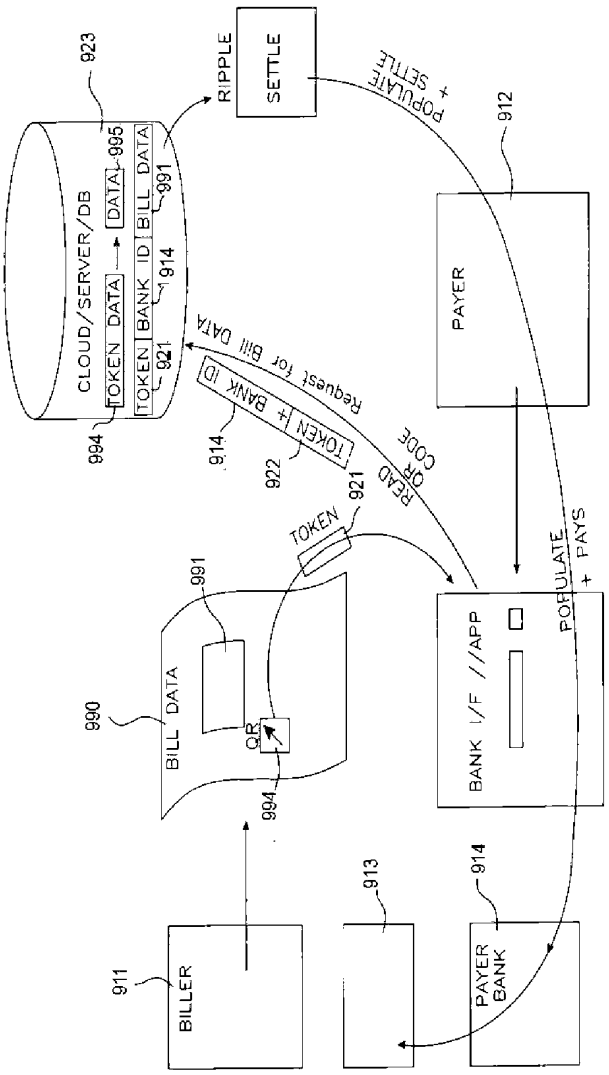

923
RIPPLE
SETTLE
POPULATE + SETTLE
912
CLOUD/SERVER/DB
DATA
995
TOKEN DATA
BANK ID
BILL DATA
991
914
921
PAYER
Request for Bill DATA
TOKEN + BANK ID
READ QR CODE
994
914
922
921
TOKEN
991
990
BILL DATA
QR
994
BANK I/F //APP
POPULATE + PAYS
913
914
911
BILLER
PAYER BANK

FIG. 9B

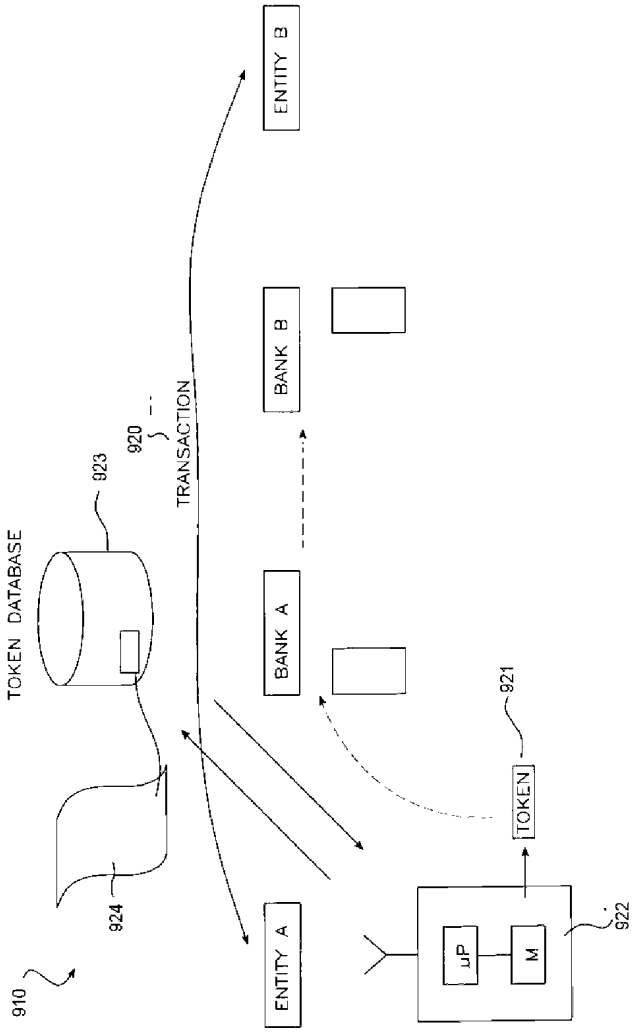

ENTITY B
BANK B
BANK A
ENTITY A
TRANSACTION
920
923
TOKEN DATABASE
924
910
921
TOKEN
922
μP
M

FIG. 9C

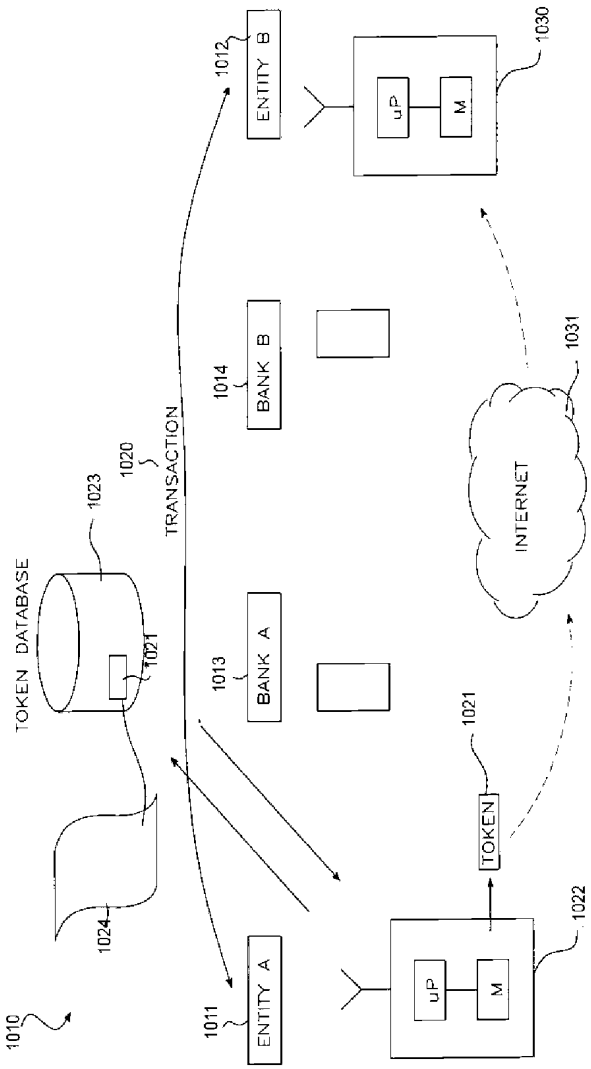

1010
1011
ENTITY A
1012
ENTITY B
1013
BANK A
1014
BANK B
1020
TRANSACTION
1021
TOKEN
1022
uP
M
1023
TOKEN DATABASE
1024
1030
1031
INTERNET

FIG. 10A

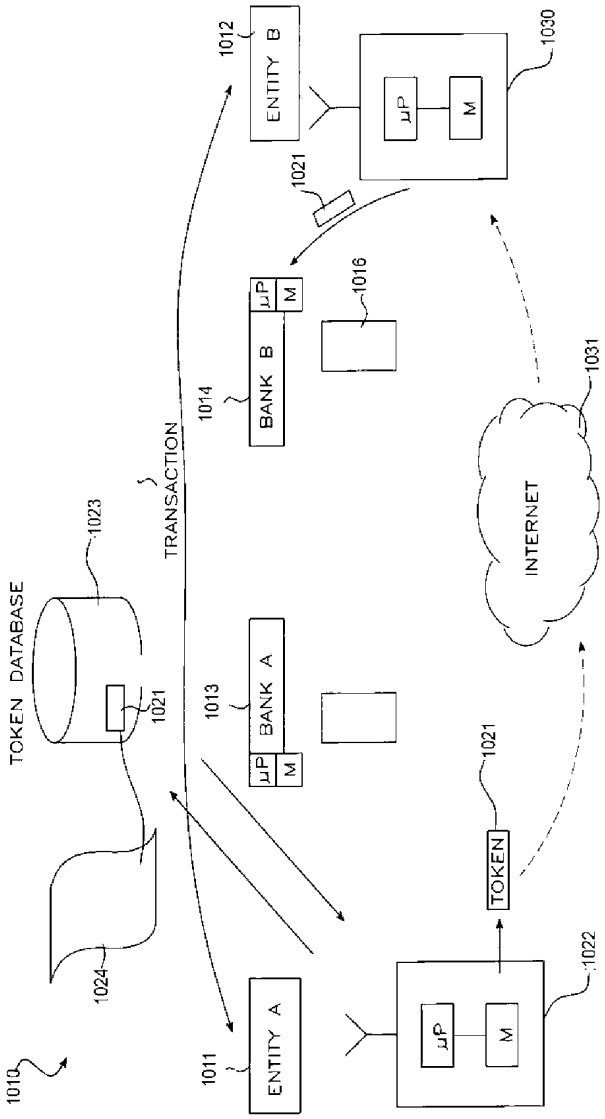

1012
ENTITY B
1030
μP
M
1021
1016
μP
M
BANK B
1014
TRANSACTION
1031
INTERNET
1023
TOKEN DATABASE
1021
1013
BANK A
μP
M
1021
TOKEN
1024
1022
μP
M
1011
ENTITY A
1010

FIG. 10B

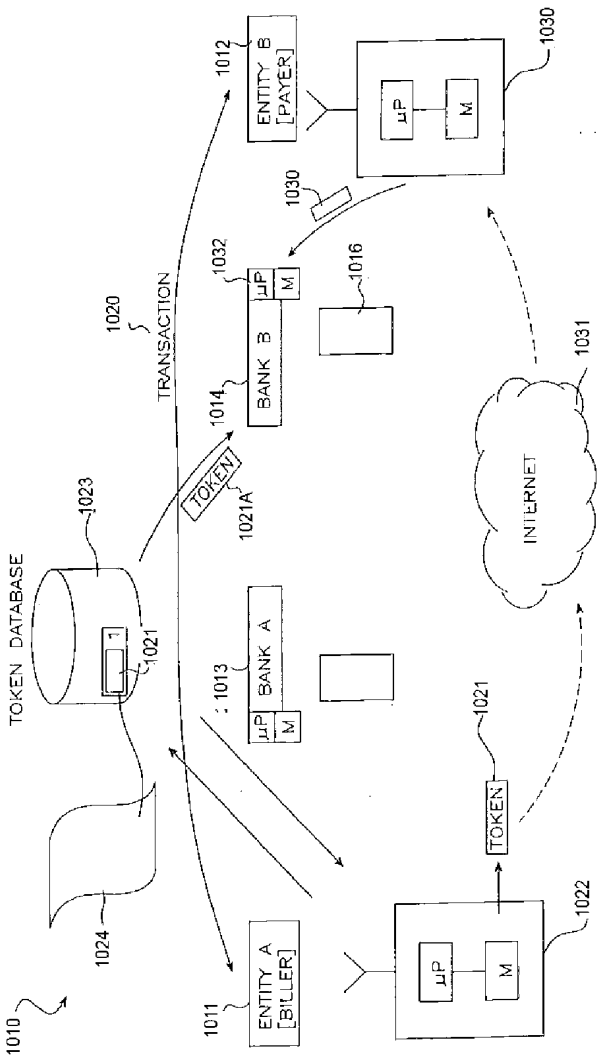

1010
1011
ENTITY A [BILLER]
1012
ENTITY B [PAYER]
1013
BANK A
1014
BANK B
1016
1020
TRANSACTION
1021
1021A
TOKEN
1022
1023
TOKEN DATABASE
1024
1030
1031
INTERNET
1032
µP
M

FIG. 10C

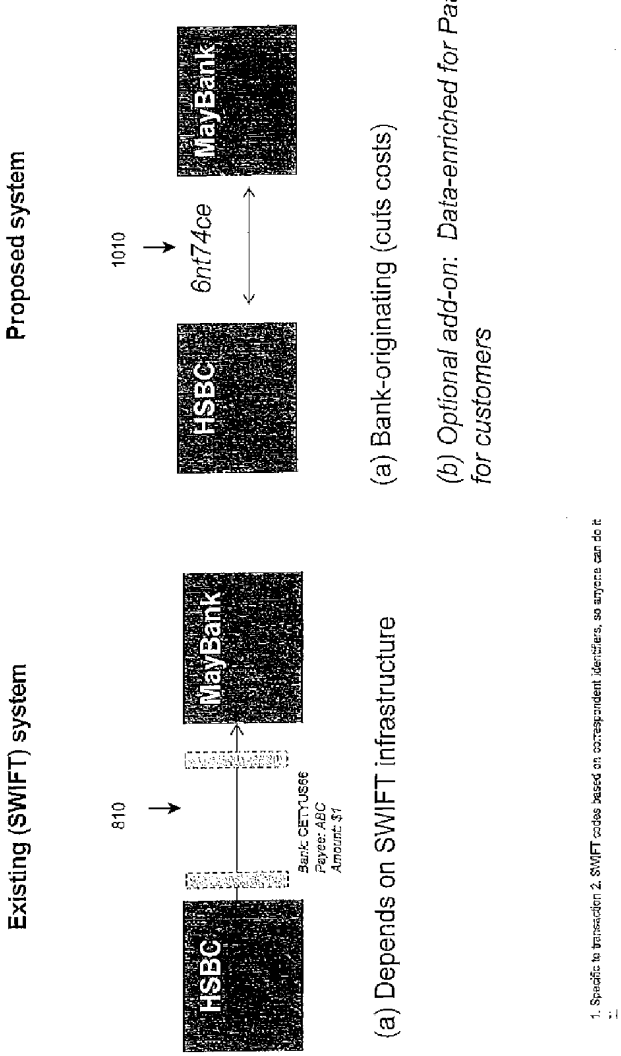

Existing (SWIFT) system
Proposed system
HSBC
MayBank
810
Bank: CITYUS66
Payee: ABC
Amount: $1
1010
6nt74ce
HSBC
MayBank
(a) Depends on SWIFT infrastructure
(a) Bank-originating (cuts costs)
(b) Optional add-on: Data-enriched for PaaS for customers
1. Specific to transaction 2. SWIFT codes based on correspondent identifiers, so anyone can do it

FIG. 11

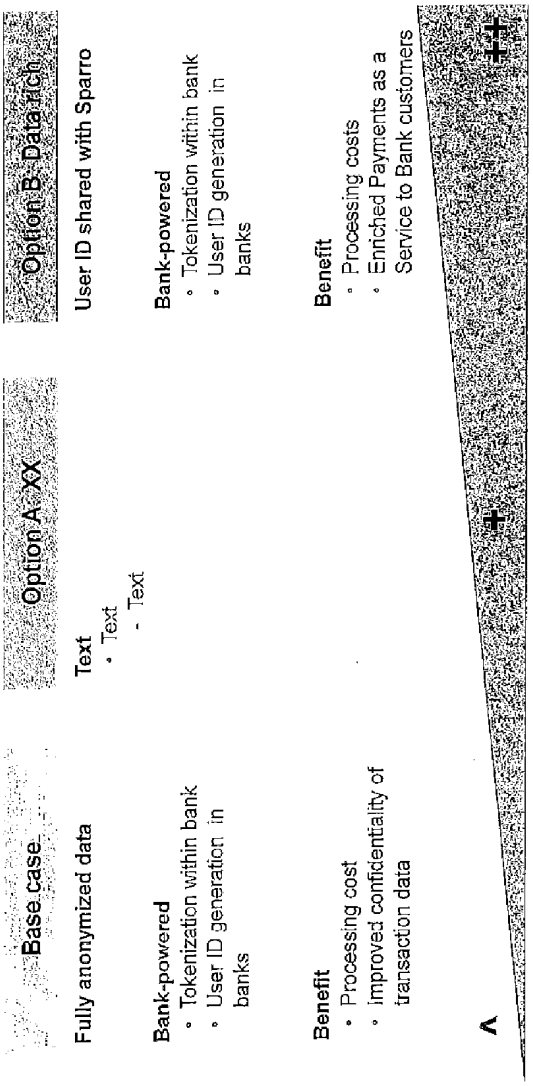

Base case
Fully anonymized data
Bank-powered
• Tokenization within bank
• User ID generation in banks
Benefit
• Processing cost
• improved confidentiality of transaction data
Option A: XX
Text
• Text
- Text
Bank-powered
• Tokenization within bank
• User ID generation in banks
Benefit
• Processing costs
• Enriched Payments as a Service to Bank customers
Option B: Data rich
User ID shared with Sparro
+
++
+++

FIG. 12

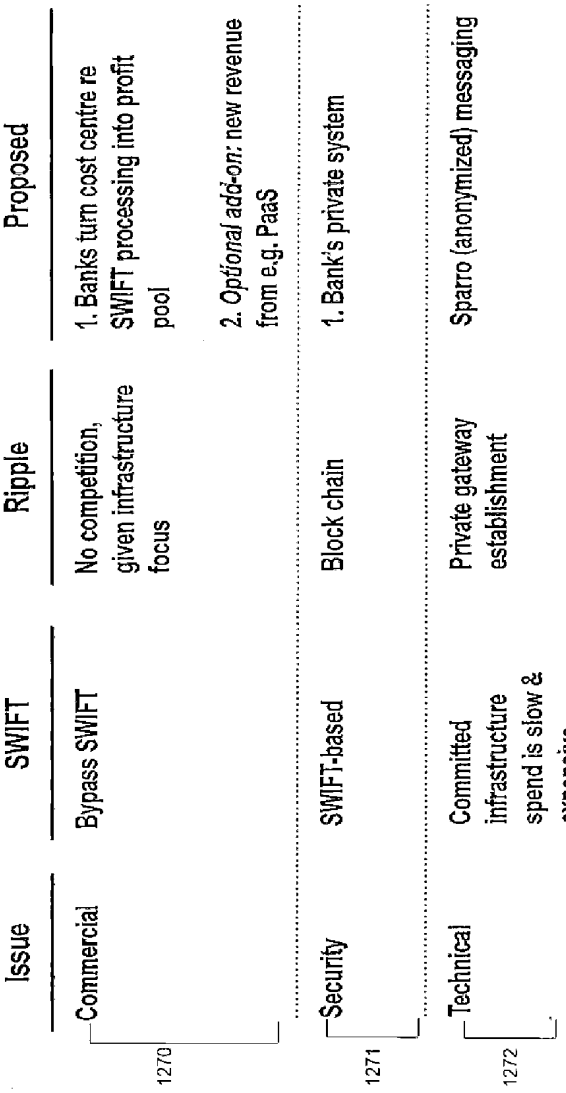

Issue
SWIFT
Ripple
Proposed
Commercial
Bypass SWIFT
No competition, given infrastructure focus
1. Banks turn cost centre re SWIFT processing into profit pool
2. Optional add-on: new revenue from e.g. PaaS
1270
Security
SWIFT-based
Block chain
1. Bank's private system
1271
Technical
Committed infrastructure spend is slow & expensive
Private gateway establishment
Sparro (anonymized) messaging
1272

FIG. 13

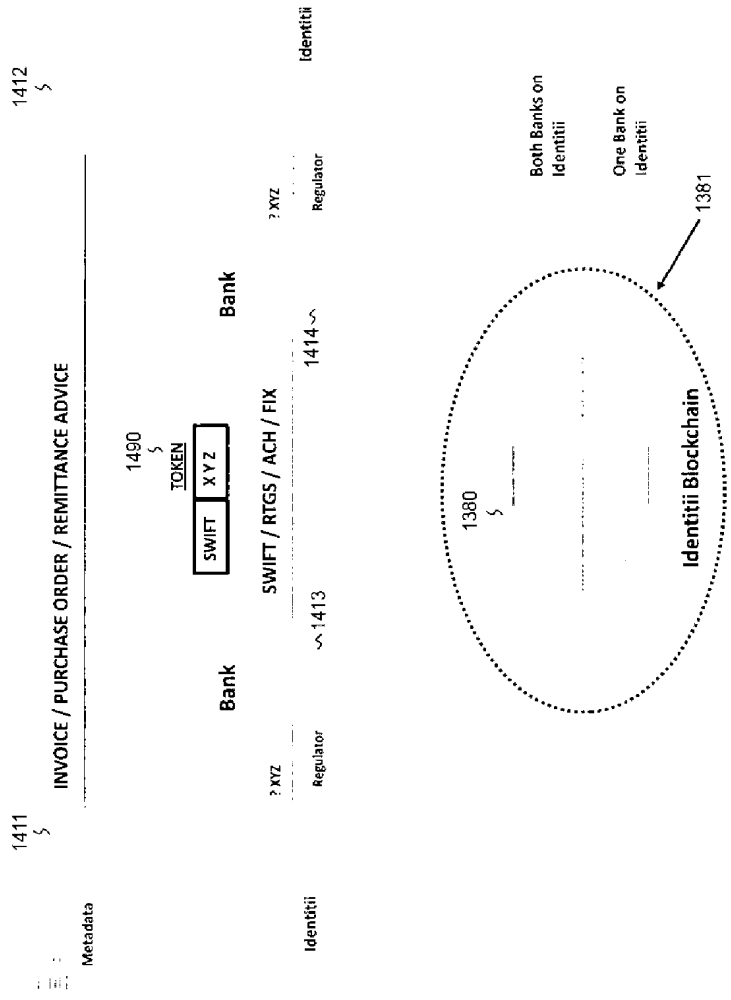

1412
INVOICE / PURCHASE ORDER / REMITTANCE ADVICE
1411
Metadata
1490
TOKEN
SWIFT
XYZ
Bank
Bank
SWIFT / RTGS / ACH / FIX
1414
1413
? XYZ
Regulator
Identitii
? XYZ
Regulator
Identitii
Both Banks on Identitii
One Bank on Identitii
1381
1380
Identitii Blockchain

FIG. 14

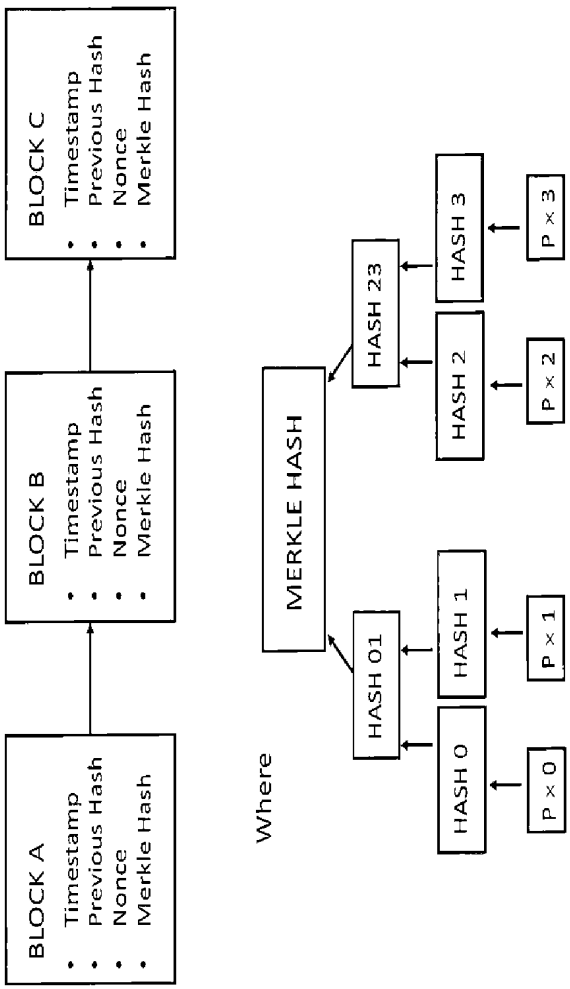

BLOCK A
Timestamp
Previous Hash
Nonce
Merkle Hash
BLOCK B
Timestamp
Previous Hash
Nonce
Merkle Hash
BLOCK C
Timestamp
Previous Hash
Nonce
Merkle Hash
Where
MERKLE HASH
HASH 23
HASH 01
HASH 2
HASH 3
HASH 1
HASH 0
P × 0
P × 1
P × 2
P × 3

FIG. 15A

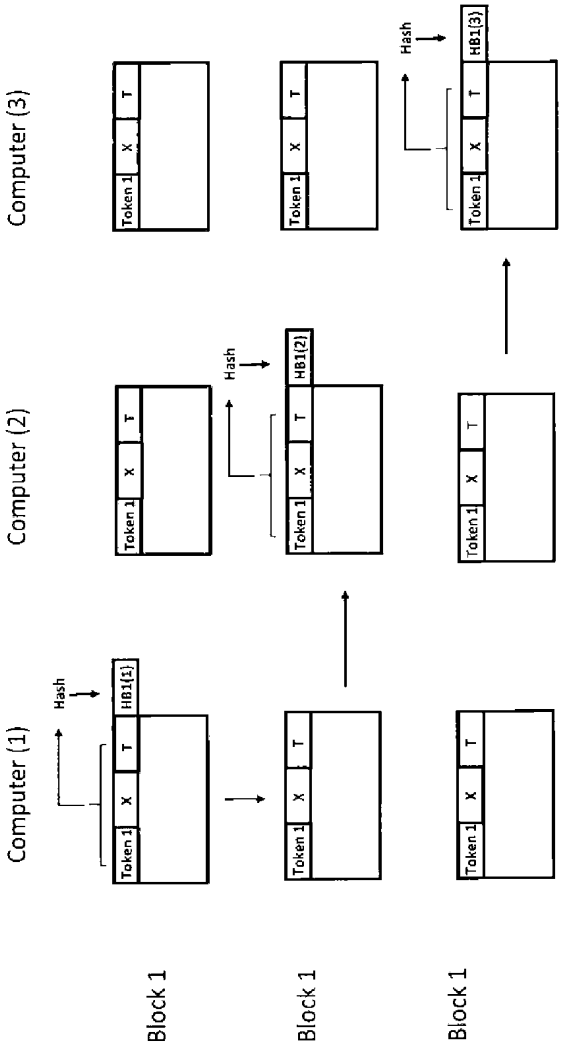

Computer (3)
Computer (2)
Computer (1)
Hash
HB1(1)
HB1(2)
HB1(3)
Token 1
X
T
Block 1
Block 1
Block 1

FIG. 15B

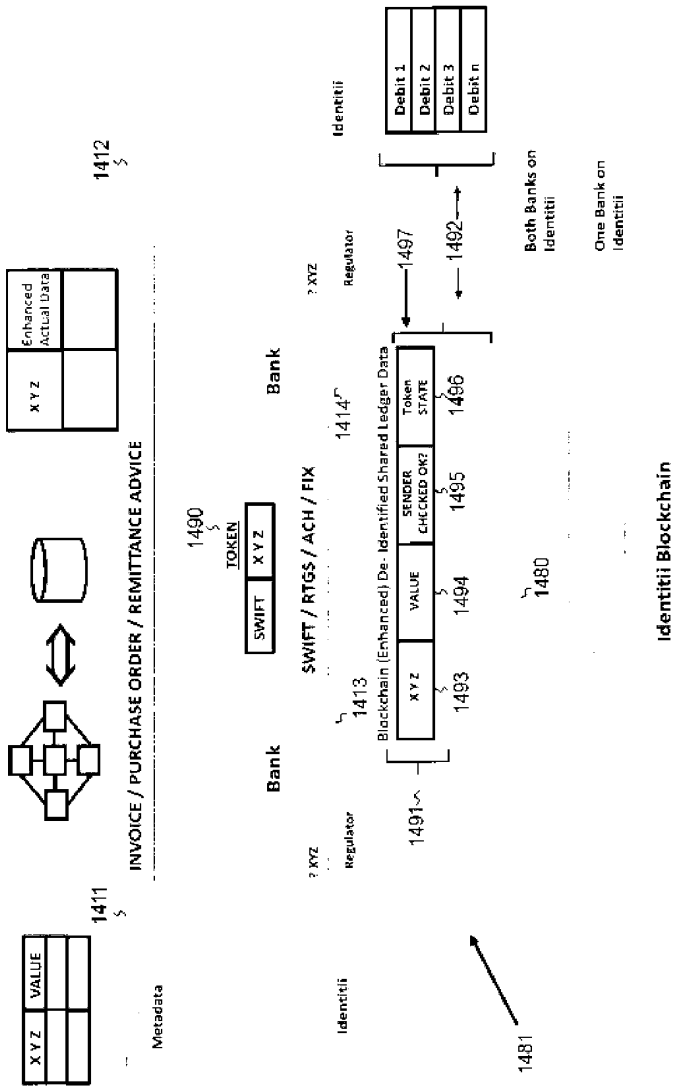

1411
XYZ
VALUE
Metadata
1412
XYZ
Enhanced Actual Data
INVOICE / PURCHASE ORDER / REMITTANCE ADVICE
1490
TOKEN
SWIFT
XYZ
SWIFT / RTGS / ACH / FIX
Bank
Bank
? XYZ
Regulator
Identitii
1413
1414
Blockchain (Enhanced) De- Identified Shared Ledger Data
XYZ
VALUE
SENDER CHECKED OK?
Token STATE
1491
1493
1494
1495
1496
1497
1492
Debit 1
Debit 2
Debit 3
Debit n
Both Banks on Identitii
One Bank on Identitii
1480
Identitii Blockchain
1481

FIG. 16

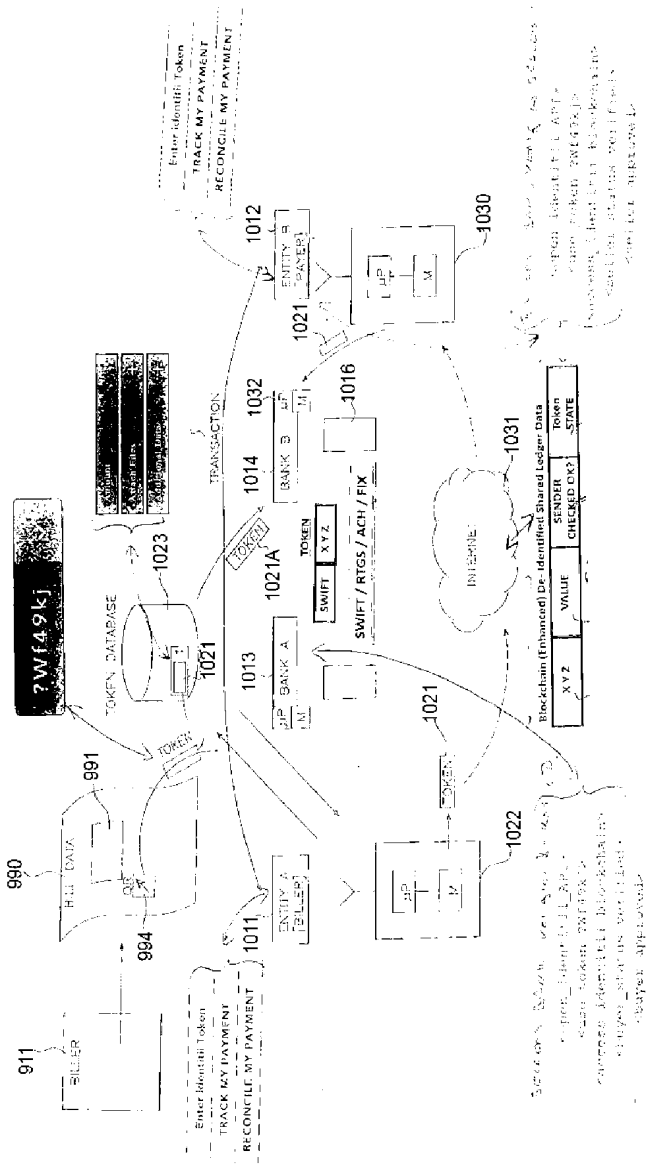

911
BILLER
990
991
994
1011
ENTITY A (BILLER)
1012
ENTITY B (PAYER)
1013
BANK A
1014
BANK B
1016
SWIFT / RTGS / ACH / FIX
1021
1021A
1022
1023
1030
1031
1032
TOKEN
TOKEN DATABASE
TRANSACTION
INTERNET
SWIFT
XYZ
VALUE
SENDER
Token
STATE
Blockchain (Enhanced) De-Identified Shared Ledger Data
Enter Identity Token
TRACK MY PAYMENT
RECONCILE MY PAYMENT

FIG. 17

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

(Chapter II of the Patent Cooperation Treaty)

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference P01740WO1	**FOR FURTHER ACTION**	See Form PCT/IPEA/416
International application No. **PCT/AU2016/000279**	International filing date *(day/month/year)* 12 August 2016	Priority date *(day/month/year)* 14 August 2015

International Patent Classification (IPC) or national classification and IPC

G06Q 20/38 (2012.01) G06F 17/30 (2006.01)

Applicant

IDENTITII PTY LTD

1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of **6** sheets, including this cover sheet.
3. This report is also accompanied by ANNEXES, comprising:
   a. [X] *(sent to the applicant and to the International Bureau)* a total of **35** sheets, as follows:
      - [X] sheets of the description, claims and/or drawings which have been amended and/or sheets containing rectifications authorized by this Authority, unless those sheets were superseded or cancelled, and any accompanying letters (see Rules 46.5, 66.8, 70.16, 91.2, and Section 607 of the Administrative Instructions).
      - [ ] sheets containing rectifications not taken into account by this Authority because they were not available at the time when this Authority began to draw up this report, and any accompanying letters (Rules 66.4*bis*, 70.2(e), 70.16 and 91.2).
      - [ ] Superseded sheets and any accompanying letters, where this Authority either considers that the superseding sheets contain an amendment that goes beyond the disclosure in the international application as filed, or the superseding sheets were not accompanied by a letter indicating the basis for the amendments in the application filed, as indicated in item 4 of Box No. I and the Supplemental Box (see Rule 70.16(b)).
   b. [ ] *(sent to the International Bureau only)* a total of (indicate type and number of electronic carrier(s)) , containing a sequence listing, in electronic form only, as indicated in the Supplemental Box Relating to Sequence Listing (see paragraph 3*bis* of Annex C of the Administrative Instructions).
4. This report contains indications relating to the following items:

[X]	Box No. I	Basis of the report
[ ]	Box No. II	Priority
[ ]	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
[ ]	Box No. IV	Lack of unity of invention
[X]	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
[ ]	Box No. VI	Certain documents cited
[ ]	Box No. VII	Certain defects in the international application
[ ]	Box No. VIII	Certain observations on the international application

Date of submission of the demand	Date of completion of this report
10 March 2017	14 December 2017
Name and mailing address of the IPEA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA Email address: pct@ipaustralia.gov.au	**Authorised officer** Peter Garay AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No. +61262832451

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.
PCT/AU2016/000279

Box No. I Basis of the report

1. With regard to the **language**, this report has been established on the basis of:

[X] The international application in the language in which it was filed:

[ ] A translation of the international application into , which is the language of a translation furnished for the purposes of :

[ ] international search (under Rules 12.3(a) and 23.1 (b)).

[ ] publication of the international application (under Rule 12.4(a)).

[ ] international preliminary examination (Rules 55.2(a) and/or 55.3(a) and (b)).

2. With regard to the **elements** of the international application, this report is based on *(replacement sheets which have been furnished to the receiving office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report)*:

[ ] the international application as originally filed/furnished, or

[X] the description: pages **1-75** , as originally filed/furnished

pages , received by this Authority on with the letter of

[X] the claims: pages , as originally filed/furnished

pages , as amended (together with any statement) under Article 19,

pages **76-91** , received by this Authority on **13 November 2017** with the letter of **13 November 2017**

[X] the drawings: pages **1/23-23/23** , as originally filed/furnished

pages , received by this Authority on with the letter of

[ ] a sequence listing - see Supplemental Box Relating to Sequence Listing.

3. [ ] The amendments have resulted in the cancellation of:

[ ] the description, pages

[ ] the claims, Nos.

[ ] the drawings, sheets/figs

[ ] the sequence listing (specify):

4. [ ] This report has been established as if (some of) the amendments annexed to this report and listed below had not been made, since either they are considered to go beyond the disclosure as filed, or they were not accompanied by a letter indicating the basis for the amendments in the application as filed, as indicated in the Supplemental Box (Rules 70.2(c) and (*c-bis*)):

[ ] the description, pages

[ ] the claims, Nos.

[ ] the drawings, sheets/figs

[ ] the sequence listing (specify):

5. [ ] This report has been established:

[ ] taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rules 66.1(d-*bis*) and 70.2(e)).

[ ] without taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rules 66.4*bis* and 70.2(e)).

6. With regard to top-up searches (Rules 66.1*ter* and 70.2(f)):

[X] A top-up search was carried out by this Authority on 7 December 2017.

[X] Additional relevant documents have been discovered during the top-up search.

[ ] No top-up search was carried out by this Authority because it would serve no useful purpose.

7. [ ] Supplementary international search report(s) from Authority(ies) has/have been received and taken into account in establishing this report (Rule 45*bis*.8(b) and (c)).

* *If item 4 applies, some or all of those sheets may be marked "superseded."*

Box No. V **Reasoned statement under Article 35(2) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims **1-50, 52-58**	**YES**
	Claims **51**	**NO**
Inventive step (IS)	Claims **NONE**	**YES**
	Claims **1-58**	**NO**
Industrial applicability (IA)	Claims **1-58**	**YES**
	Claims **NONE**	**NO**

2. CITATIONS AND EXPLANATIONS:

CITATIONS

D1: WO 2015/116998 A2 (KREMEN) 06 August 2015

D2: US 2009/0100041 A1 (WILSON) 16 April 2009

D3: US 2011/0184910 A1 (LOVE et al.) 28 July 2011

D4: EP 2843587 A1 (OPENLIMIT SIGNCUBES AG) 04 March 2015

D5: US 2004/0006692 A1 (HONDA et al.) 08 January 2004

D6: US 2008/0201580 A1 (SAVITZKY et al.) 21 August 2008

D7: Snow, P., et al. "Factom Ledger by Consensus." [retrieved from internet on 25 October 2016]. < URL: http://bravenewcoin.com/assets/Whitepapers/FactomLedgerbyConsensus.pdf > (The International Searching Authority is unable to establish the publication date of the above citation).

D8: Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008). [retrieved from internet on 25 October 2016]. < URL: http://web.archive.org/web/20150616021417/http://www.cryptovest.co.uk/resources/Bitcoin%20paper%20Original.pdf > published on or before 16 June 2015 as per Wayback Machine

D9: US 2014/0279519 A1 (JUMIO INC) 18 September 2014

NOVELTY (N)

Note: D9 - new citation

Claim 51:

D9 discloses a second intermediary server for use in a centralised financial system to facilitate processing of a financial transaction [0023, 0031], operably connected to a network and a second document store (fig 1), and configured to:

- receive the token from the second digital device (fig 1, [0024, 0033];
- transmit the token to the second document store [0041]; and

JPMC Ex. 1002
Page 824

- send a second financial message comprising the token to a first intermediary server in the centralised financial system, indicative of making a payment to a first user (this step is a confirmation which is an inherent step in a centralised (legacy) financial system, see payments methods at [0068]).

Therefore the subject matter of claim 51 is not new and does not meet the requirements of Article 33(2) of the PCT with regard to novelty.

Claims 1-50, 52-58:

None of the cited art is discussing the features of these claims, in particular the use of a blockchain in conjunction with a document store to supplement a centralised financial system in relation to document handling.

The subject matter of claims 1-50 and 52-58 is new and meets the requirements of Article 33(2) of the PCT with regard to novelty.

INVENTIVE STEP (IS)

Claim 51:

Claim 51 considered to lack an inventive step for the same reasons as discussed in relation to lack of novelty above.

Claim 1:

Document D9 is on the topic of providing and sharing identity information and documents and therefore is considered to be the closest prior art in the field.

D9 discloses a computer implemented method for processing a financial transaction, the method comprising the steps of:

- transmitting one or more documents pertaining to the financial transaction [0023, 0031], from a first intermediary ~~server in~~ a centralised financial system to a first document store (610 on Fig 6);
- generating an enriched data record from the one or more documents, at the first intermediary server, and adding the enriched data record into ~~a blockchain being a distributed ledger~~, from the first intermediary ~~sever~~ [0026, 0036];
- requesting generation of a token corresponding to the financial transaction to identify the one or more documents, to a token server, from the first intermediary ~~server~~, via a messaging bus in the centralised financial system [0033];
- generating the token at the token server and adding the token into ~~the blockchain~~ from the token server in association with the enriched data record [0036, 0037];
- transmitting the token to the first intermediary server from the token server, via the messaging bus [0051] ; and
- transmitting the token from the first intermediary ~~server~~ to the first document store in association with the one or more documents [0029].

The term "messaging bus" is read in the context of the claim to be any mechanism to allow the particular information flow according to the logic of the claim.

The invention therefore differs to what has been disclosed in the following:

JPMC Ex. 1002
Page 825

- Access to the first document store is via a decentralised system rather than being accessed by a centralised system. Accessing the first store remotely as opposed to via a centralised system is merely due to the workflow used to collect the document image, and either option can be implemented by a person skilled in the art without any difficulty. The workflow claimed in your application starts with an institution having the document, while the workflow in D9 starts with the user providing the document. The workflow according to disclosure of D9 makes it possible for a user device to be registered as an identification device, but such a feature is clearly optional. If the use of the user device for identification is not utilized, it is obvious to make that change to what is disclosed in D9 to replace the workflow that is initiated by a user with an alternative workflow that is initiated remotely without invention.

- Additionally in your application a data record and a token is entered into a blockchain. While this feature is not disclosed in the prior art, adding additional information into the blockchain is merely utilising an alternative way to store information.

Neither of these differences are considered to involve an inventive step.

Claims 2 , 4 and 8:

The additional features of these claims are directly derivable from the business logic relating to the subject matter, namely of providing and sharing identity information and documents.

Claim 3:

Being able to store a smart contract is known feature of a blockchain, see discussion in D7.

Claim 5:

D9 discloses a computer implemented method as claimed in claim 1, wherein the step of generating the enriched data record comprises:

- extracting a plurality of attributes from the one or more documents, at the first intermediary server [0045]; and

- combining the plurality of attributes to generate the enriched data record, at the first intermediary server [0048].

Claims 6 and 7:

D9 discloses the hashing (and consequently de-identifying) of multiple attributes [0046].

Claims 9-11 and 13-16:

The additional features of these claims are features are inherent in using the Bitcoin blockchain distributed trustless ledger systems.

Claims 12 ,17, 29, 34, 45 and 58:

The features of this claim relate to the specific document type manipulated as part of a transaction. There is nothing disclosed that would indicate that regulatory compliance documents have any specific feature that would require any sort problem to be overcome to be manipulated. This feature is merely a specific use that would be implemented as a matter routine by a person skilled in the art. Furthermore it is considered that KYC (Know Your Customer) documents are regulatory compliance documents, disclosed in D9 at [0023].

Claims 18-20, 22-25, 27, 28 and 31-33:

JPMC Ex. 1002
Page 826

These claims have features analogous to claims 1-3, 5-8, 10, 11 and 14-16 respectively, therefore the same remarks apply, mutatis mutandis.

Claims 21, 26 and 30:

The additional features of claims are inherent in using a blockchain.

Claim 35:

The features of this claim is a subset of the features of claim 1, therefore the same remarks apply, mutatis mutandis.

Claim 36:

This claim has features analogous to claim 3, therefore the same remarks apply, mutatis mutandis.

Claims 37, 38, 40-44 and 46-50:

These claims have features analogous to claims 1 [37], 2 [38], 5-8 [40-43], 9 (in part) [44], 10 [46], 11 (in part) [47], 30 (in part) [48], 32 (in part) [49], 33 (in part) [50], respectively, therefore the same remarks apply, mutatis mutandis.

Claim 39:

D9 discloses the first intermediary server as claimed in claim 37, further configured to transmit the token to a first digital device [0040].

Claims 52 and 53:

The features of these claim are a subset of the features of claims 9 and 11, therefore the same remarks apply, mutatis mutandis.

Claims 54-57:

The features of these claim are a subset of the features of claims 13-16, therefore the same remarks apply, mutatis mutandis.

Therefore the subject matter of claims 1-58 is obvious and does not meet the requirements of Article 33(3) of the PCT with regard to inventive step.

INDUSTRIAL APPLICABILITY (IA)

The invention defined in the claims is considered to meet the requirements of Industrial Applicability under Article 33(4) of the PCT because it can be made by, or used in, industry.

JPMC Ex. 1002
Page 827

BaxterIP®
Patent Attorneys

Sydney: Suite 2, Level 3A, 1 Bligh St
+61 02 9264 6716

Melbourne: Suite 803, Level 8, 488 Bourke St
+61 03 9602 2288

Brisbane: Level 10, 239 George St
+61 07 3188 5624

Adelaide: Technology Park, 1284 South Rd
Clovelly Park
+61 08 7078 0174

Mailing Address: 1 Bligh St, Sydney NSW 2000

Email: mail@baxterip.com.au
Web: www.BaxterIP.com.au

International Preliminary Examination Authority
IP Australia
PO Box 200
Woden ACT, 2606
Australia

13 November 2017
By eServices

Our Ref: P01740WO1

Confidential

Subject: Response to written opinion
Application No.: PCT/AU2016/000279
In the Name of: Identitii Pty Ltd
Entitled: A COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR

Dear Examiner,

In response to the Written Opinion of the International Preliminary Examining Authority issued on the above PCT application on 13 October 2017, we respectfully submit our arguments below and the proposed amendments to the claims as attached.

Novelty and inventiveness

To facilitate the Examiner's understanding of the present invention and D1, we provided a brief background description in relation to the present invention and D1 in our response to the previous Written Opinion, which was submitted on 12 September 2017, particularly, see the section "Background of the present invention and D1 (WO2015/116998 A2 (KREMEN))" in the previous response.

As set out in the Background section, the present invention has some distributed electronic transfer attributes by introducing the token and blockchain but works with the centralised banking system to take advantage of the capabilities of the conventional messaging system provided by the centralised banking systems, while D1 is directed to a completely decentralised electronic transfer system 200 with distribution control capability, as shown in Fig. 2 and described in paragraph [0018] of D1. The claims were also amended accordingly.

However, the Examiner has alleged in this written opinion that the amendments made in the previous response did not require such limitation. Although we disagree with the Examiner, we have further amended independent claims to emphasise the unique aspect of this invention. The amended independent claim 1 is recited below for easy reference:

1. *A computer implemented method for processing a financial transaction, the method comprising the steps of:*
   transmitting one or more documents pertaining to the financial transaction, from a first intermediary server <u>in a centralised financial system</u> to a first document store;

generating an enriched data record from the one or more documents, at the first intermediary server, and adding the enriched data record into a blockchain being a distributed ledger, from the first intermediary sever;

requesting generation of a token corresponding to the financial transaction to identify the one or more documents, to a token server, from the first intermediary server, via a messaging bus in the centralised financial system;

generating the token at the token server and adding the token into the blockchain from the token server in association with the enriched data record;

transmitting the token to the first intermediary server from the token server, via the messaging bus; and

transmitting the token from the first intermediary server to the first document store in association with the one or more documents.

In the Written Opinion, the rules of D1 are interpreted by the Examiner as the "one or more documents pertaining to the financial transaction" of claim 1. However, paragraph [0014] of D1 merely discloses that the rules can be inserted into each electronic transfer without particularly disclosing "*from a first intermediary server in a centralised financial system to a first document store*" as claimed in the amended claim 1. As claimed in claim 1, the first intermediary server and the first document store are different from the blockchain "*being a distributed ledger*". In fact, as described throughout the present specification, particularly, paragraphs [0089] and [0090] of the present specification, the first intermediary server is part of a centralised financial system. This is how the present invention takes advantage of the centralised financial system. As D1 is directed to the completely decentralised electronic transfer system 200 (i.e., a distributed ledger), D1 does not interact with a centralised financial system to modify the transfer request. Therefore, the rules of D1 are actually transferred within the decentralised electronic transfer system 200 instead of being transferred "*from a first intermediary server in a centralised financial system to a first document store*".

Secondly, D1 fails to disclose "*generating an enriched data record from the one or more documents, at the first intermediary server, and adding the enriched data record into a blockchain being a distributed ledger, from the first intermediary server*" as claimed in claim 1. As analysed above, D1 does not interact with the centralised financial system to modify the transfer request. Therefore, it is not possible that D1 generates the enriched data "*at the first intermediary server*", which is part of the centralised financial system as claimed in claim 1.

Thirdly, D1 fails to disclose "*requesting generation of a token corresponding to the financial transaction to identify the one or more documents, to a token server, from the first intermediary server, via a messaging bus in the centralised financial system*". Even if D1 generates a token, as D1 is directed to the completely decentralised blockchain system 200, D1 does not request the token "*from the first intermediary server, via a messaging bus in the centralised financial system*" as claimed in the amended claim 1, in which both the first intermediary sever and the messaging bus are part of the centralised financial system and outside the blockchain.

In the fourth integer of claim 1, D1 fails to disclose "*generating the token at the token server and adding the token into the blockchain from the token server in association with the enriched data record*". The Examiner appears to have contradicted himself in that if the verified data in paragraph [0018] is considered to be a token as the Examiner suggests, then the timestamp cannot also be considered a token as the Examiner has suggested.

Furthermore, the Examiner has asserted that the feature of "*transmitting the token to the first intermediary server from the token server, via the messaging bus*" is disclosed in D1. The Examiner has used the argument that Fig. 2 of D1 discloses a "modified (verified) ruleset is stored back in the block chain". Again, D1 is directed to the completely decentralised blockchain system 200 and does not interact with a centralised financial system to modify the transfer request. Therefore, D1 does not transfer the token between the first intermediary server in the centralised financial system and the token server via the messaging bus in the centralised financial system.

Finally, in relation to the last integer of claim 1, the Examiner asserts that D1 discloses "*transmitting the token from the first intermediary server to the first document store in association with the one or*

more documents". Again, D1 is directed to the completely decentralised blockchain system 200 and does not interact with a centralised financial system to modify the transfer request. Therefore, D1 does not transfer the token between the first intermediary server in the centralised financial system and the first document store.

Based on the above analysis, the amended independent claim 1 is novel and inventive with respect to D1. Since similar amendments have been made to other independent claims 18, 35, 37, 51, 52 and 54, the similar arguments are also applicable to these amended independent claims. Given novelty and inventiveness of independent claims 1, 18, 35, 37, 51, 52 and 54, dependent claims in the claim set are novel and inventive by virtue of their dependencies on the independent claims.

Yours sincerely,

QI ZHANG
Registered Patent Attorney

Claims

1. A computer implemented method for processing a financial transaction, the method comprising the steps of:

transmitting one or more documents pertaining to the financial transaction, from a first intermediary server in a centralised financial system to a first document store;

generating an enriched data record from the one or more documents, at the first intermediary server, and adding the enriched data record into a blockchain being a distributed ledger, from the first intermediary sever;

requesting generation of a token corresponding to the financial transaction to identify the one or more documents, to a token server, from the first intermediary server, via a messaging bus in the centralised financial system;

generating the token at the token server and adding the token into the blockchain from the token server in association with the enriched data record;

transmitting the token to the first intermediary server from the token server, via the messaging bus; and

transmitting the token from the first intermediary server to the first document store in association with the one or more documents.

2. The computer implemented method as claimed in claim 1, further comprising the step of sending a first financial message comprising the token, from the first intermediary server to a second intermediary server in the centralised financial system, indicative of making a payment to a second user.

3. The computer implemented method as claimed in claim 1, further comprising the steps of:

implementing a smart contract at the token server; and

adding the smart contract into the blockchain, from the token server.

4. The computer implemented method as claimed in claim 1, further comprising the steps of:

transmitting the token from the first intermediary server to a first digital device available with a first user;

providing the token to a second user, by the first user;

providing the token to a second intermediary server in the centralised financial system, from the second digital device;

transmitting the token to a second document store, from the second intermediary server; and

sending a second financial message comprising the token, from the second intermediary server to the first intermediary server, indicative of making a payment to the first user.

5. The computer implemented method as claimed in claim 1, wherein the step of generating the enriched data record comprises:

extracting a plurality of attributes from the one or more documents, at the first intermediary server; and

combining the plurality of attributes to generate the enriched data record, at the first intermediary server.

6. The computer implemented method as claimed in claim 1, wherein the step of generating the enriched data record comprises:

extracting a plurality of attributes from the one or more documents, at the first intermediary server;

de-identifying the plurality of attributes to obtain a plurality of de-identified attributes, at the first intermediary server; and

combining the plurality of de-identified attributes to generate the enriched data record, at the first intermediary server.

7. The computer implemented method as claimed in claim 1, wherein the step of generating the enriched data record comprises:

extracting a plurality of attributes from the one or more documents, at the first intermediary server;

hashing the plurality of attributes to generate a plurality of respective hashes, at the first intermediary server; and

combining the plurality of hashes to generate the enriched data record, at the first intermediary server.

8. The computer implemented method as claimed in claim 1, further comprising the step of assigning a payment risk rating to the token.

9. The computer implemented method as claimed in claim 1, further comprising the steps of:

transmitting one or more first requests, each comprising the token, from the first intermediary server to a second intermediary server in the centralised financial system, via the messaging bus;

receiving the one or more first requests at the second intermediary server and transmitting the one or more first requests and the token from the second intermediary server to a second document store;

generating one or more first responses, each comprising the token, corresponding to the respective one or more first requests, at the second intermediary server;

transmitting the one or more first responses from the second intermediary server to the first intermediary server, via the messaging bus;

hashing the one or more first requests and the one or more first responses at the second intermediary server to generate one or more first request hashes and one or more first response hashes, respectively;

adding the one or more first request hashes and the one or more first response hashes to the enriched data record in the blockchain, from the second intermediary server; and

receiving the one or more first responses at the first intermediary server and transmitting the one or more first responses to the first document store.

10. The computer implemented method as claimed in claim 9, further comprising the steps of:

hashing the one or more first responses at the first intermediary server to regenerate the one or more first response hashes; and

verifying the one or more first response hashes with the blockchain from the first intermediary server, using the token.

11. The computer implemented method as claimed in claim 9, wherein each one of the one or more first requests are:

encrypted with a second public key and signed with a first public key at the first intermediary server, before transmission to the second intermediary server; and

decrypted with a second private key at the second intermediary server after reception from the first intermediary server; and

wherein each one of the one or more first responses are:

encrypted with the first public key and signed with the second public key at the second intermediary server, before transmission to the first intermediary server; and

decrypted with a first private key at the first intermediary server after reception from the second intermediary server.

12. The computer implemented method as claimed in claim 9, wherein the one or more first responses comprise one or more second regulatory compliance documents pertaining to a second user.

13. The computer implemented method as claimed in claim 1, further comprising the steps of:

transmitting one or more second requests, each comprising the token, from a second intermediary server in the centralised financial system to the first intermediary server, via the messaging bus;

receiving the one or more second requests at the first intermediary server and transmitting the one or more second requests from the first intermediary server to the first document store;

generating one or more second responses, each comprising the token, corresponding to the respective one or more second requests, at the first intermediary server;

transmitting the one or more second responses from the first intermediary server to the second intermediary server, via the messaging bus;

hashing the one or more second requests and the one or more second responses at the first intermediary server to generate one or more

JPMC Ex. 1002
Page 834

second request hashes and one or more second response hashes, respectively;

adding the one or more second request hashes and the one or more second response hashes to the enriched data record in the blockchain, from the first intermediary server; and

receiving the one or more second responses at the second intermediary server and transmitting the one or more second responses to the second document store.

14. The computer implemented method as claimed in claim 13, further comprising the steps of:

hashing the one or more second responses at the second intermediary server to regenerate the one or more second response hashes; and

verifying the one or more second response hashes with the blockchain from the second intermediary server, using the token.

15. The computer implemented method as claimed in claim 13, wherein each one of the one or more second requests are:

encrypted with a first public key and signed with a second public key at the second intermediary server, before transmission to the first intermediary server; and

decrypted with a first private key at the first intermediary server after reception from the second intermediary server; and

wherein each one of the one or more second responses are:

encrypted with the second public key and signed with the first public key at the first intermediary server, before transmission to the second intermediary server; and

decrypted with a second private key at the second intermediary server after reception from the first intermediary server.

16. The computer implemented method as claimed in claim 11 or 15, further comprising the steps of adding the first public key from the first intermediary server into the blockchain and adding the second public key from the second intermediary server into the blockchain.

17. The computer implemented method as claimed in claim 13, wherein the one or more second responses comprise one or more first regulatory compliance documents pertaining to a first user.

18. A system for processing a financial transaction, the system comprising:

a first intermediary server in a centralised financial system, the first intermediary server being operably connected to a network and a first document store;

a token server operably connected to the network;

a messaging bus in the centralised financial system, the messaging bus being operably connected to the network; and

a blockchain operably connected to the network, the blockchain being a distributed ledger;

wherein the first intermediary server is configured to:

transmit one or more documents pertaining to the financial transaction, to the first document store;

generate an enriched data record from the one or more documents and add the enriched data record into the blockchain;

request generation of a token corresponding to the financial transaction to identify the one or more documents, to the token server, via the messaging bus; and

transmit the token to the first document store;

wherein the token server is configured to:

generate the token and add the token into the blockchain in association with the enriched data record; and

transmit the token to the first intermediary server, via the messaging bus.

19. The system as claimed in claim 18, further comprising a second intermediary server in the centralised financial system, operably connected to the network and a second document store;

wherein the first intermediary server is further configured to send a first financial message comprising the token, to the second intermediary server, indicative of making a payment to a second user.

20. The system as claimed in claim 18, wherein the token server is further configured to:

implement a smart contract; and

add the smart contract into the blockchain.

21. The system as claimed in claim 18, further comprising:

a first digital device operably connected to the network;

a second digital device operably connected to the network;

a second intermediary server in the centralised financial system, the second intermediary server being operably connected to the network and a second document store;

wherein the first intermediary server is further configured to:

transmit the token to the first digital device;

wherein the first digital device comprises a first memory and a first processor operably connected to the first memory, the first memory comprising a first computer program code, the first computer program code when executed by the first processor, instructs the first processor to:

receive the token from the first intermediary server;

provide the token to the second digital device;

wherein the second digital device comprises a second memory and a second processor operably connected to the second memory, the second memory comprising a second computer program code, the second computer program code when executed by the second processor, instructs the second processor to:

receive the token from the first digital device; and

provide the token to the second intermediary server; and

wherein the second intermediary server is configured to:

receive the token from the second digital device;

transmit the token to the second document store; and

send a second financial message comprising the token, to the first intermediary server, indicative of making a payment to a first user.

22. The system as claimed in claim 18, wherein for generation of the enriched data record, the first intermediary server is configured to:

extract a plurality of attributes from the one or more documents; and

combine the plurality of attributes to generate the enriched data record.

23. The system as claimed in claim 18, wherein for generation of the enriched data record, the first intermediary server is configured to:

extract a plurality of attributes from the one or more documents;

de-identify the plurality of attributes to obtain a plurality of de-identified attributes; and

combine the plurality of de-identified attributes to generate the enriched data record.

24. The system as claimed in claim 18, wherein for generation of the enriched data record, the first intermediary server is configured to:

extract a plurality of attributes from the one or more documents;

hash the plurality of attributes to generate a plurality of respective hashes; and

combine the plurality of hashes to generate the enriched data record.

25. The system as claimed in claim 18, wherein the first intermediary server is further configured to assign a payment risk rating to the token.

26. The system as claimed in claim 18, further comprising:

a second intermediary server in the centralised financial system, the second intermediary server being operably connected to the network and a second document store;

wherein the first intermediary server is configured to:

transmit one or more first requests, each comprising the token, to the second intermediary server, via the messaging bus; and

receive one or more first responses and transmit the one or more first responses to the first document store;

wherein the second intermediary server is configured to:

receive the one or more first requests from the first intermediary server and transmit the one or more first requests and the token to the second document store;

generate the one or more first responses, each comprising the token, corresponding to the respective one or more first requests;

transmit the one or more first responses to the first intermediary server, via the messaging bus;

hash the one or more first requests and the one or more first responses to generate one or more first request hashes and one or more first response hashes, respectively; and

add the one or more first request hashes and the one or more first response hashes to the enriched data record in the blockchain.

27. The system as claimed in claim 26, wherein the first intermediary server is further configured to:

hash the one or more first responses to regenerate the one or more first response hashes; and

verify the one or more first response hashes with the blockchain, using the token.

28. The system as claimed in claim 26, wherein the first intermediary server is further configured to:

encrypt each one of the one or more first requests with a second public key and sign each one of the one or more first requests with a first public key, before transmission to the second intermediary server; and

decrypt each one of the one or more first responses with a first private key after reception from the second intermediary server;

wherein the second intermediary server is further configured to:

encrypt the each one of the one or more first responses with the first public key and sign the each one of the one or more first

responses with the second public key, before transmission to the first intermediary server; and

decrypt the each one of the one or more first requests with a second private key after reception from the first intermediary server.

29. The system as claimed in claim 26, wherein the one or more first responses comprise one or more second regulatory compliance documents pertaining to a second user.

30. The system as claimed in claim 18, further comprising:

a second intermediary server in the centralised financial system, the second intermediary server being connected to the network and a second document store;

wherein the second intermediary server is configured to:

transmit one or more second requests, each comprising the token, to the first intermediary server, via the messaging bus;

receive one or more second responses and transmit the one or more second responses to the second document store;

wherein the first intermediary server is further configured to:

receive the one or more second requests and transmit the one or more second requests to the first document store;

generate the one or more second responses, each comprising the token, corresponding to the respective one or more second requests;

transmit the one or more second responses to the second intermediary server, via the messaging bus;

hash the one or more second requests and the one or more second responses to generate one or more second request hashes and one or more second response hashes, respectively; and

add the one or more second request hashes and the one or more second response hashes to the enriched data record in the blockchain.

31. The system as claimed in claim 30, wherein the second intermediary server is further configured to:

hash the one or more second responses to regenerate the one or more second response hashes; and

verify the one or more second response hashes with the blockchain, using the token.

32. The system as claimed in claim 30, wherein the second intermediary server is further configured to:

encrypt each one of the one or more second requests with a first public key and sign each one of the one or more second requests with a second public key, before transmission to the first intermediary server; and

decrypt each one of the one or more second responses with a second private key after reception from the first intermediary server;

wherein the first intermediary server is further configured to:

encrypt the each one of the one or more second responses with the second public key and sign the each one of the one or more second responses with the first public key, before transmission to the second intermediary server; and

decrypt the each one of the one or more second requests with a first private key after reception from the second intermediary server.

33. The system as claimed in claim 28 or 32, wherein the first intermediary server is further configured to add the first public key into the blockchain and the second intermediary server is further configured to add the second public key into the blockchain.

34. The system as claimed in claim 30, wherein the one or more second responses comprise one or more first regulatory compliance documents pertaining to a first user.

35. A token server for facilitating processing of a financial transaction, operably connected to a network and configured to generate a token, add the token into a blockchain being a distributed ledger and transmit the token to a first intermediary server in a centralised financial system, via a messaging bus in the centralised financial system.

36. The token server as claimed in claim 35, further configured to:

implement a smart contract; and

add the smart contract into the blockchain

37. A first intermediary server for use in a centralised financial system to facilitate processing of a financial transaction, operably connected to a network and a first document store, and configured to:

transmit one or more documents pertaining to the financial transaction, to the first document store;

generate an enriched data record from the one or more documents and add the enriched data record into a blockchain being a distributed ledger;

request generation of a token corresponding to the financial transaction to identify the one or more documents, to a token server, via a messaging bus in the centralised financial system; and

transmit the token to the first document store.

38. The first intermediary server as claimed in claim 37, further configured to send a first financial message comprising the token, to a second intermediary server in the centralised financial system, indicative of making a payment to a second user.

39. The first intermediary server as claimed in claim 37, further configured to transmit the token to a first digital device.

40. The first intermediary server as claimed in claim 37, wherein for generation of the enriched data record, the first intermediary server is configured to:

extract a plurality of attributes from the one or more documents; and

combine the plurality of attributes to generate the enriched data record.

41. The first intermediary server as claimed in claim 37, wherein for generation of the enriched data record, the first intermediary server is configured:

extract a plurality of attributes from the one or more documents;

de-identify the plurality of attributes to obtain a plurality of de-identified attributes; and

combine the plurality of de-identified attributes to generate the enriched data record.

42. The first intermediary server as claimed in claim 37, wherein for generation of the enriched data record, the first intermediary server is configured to:

extract a plurality of attributes from the one or more documents;

hash the plurality of attributes to generate a plurality of respective hashes; and

combine the plurality of hashes to generate the enriched data record.

43. The first intermediary server as claimed in claim 37, further configured to assign a payment risk rating to the token.

44. The first intermediary server as claimed in claim 37, further configured to:

transmit one or more first requests, each comprising the token, to a second intermediary server in the centralised financial system, via the messaging bus; and

receive one or more first responses from the second intermediary server and transmit the one or more first responses to the first document store.

45. The first intermediary server as claimed in claim 44, wherein the one or more first responses comprise one or more second regulatory compliance documents pertaining to a second user.

46. The first intermediary server as claimed in claim 44, further configured to:

hash the one or more first responses to regenerate one or more first response hashes; and

verify the one or more first response hashes with the blockchain, using the token.

47. The first intermediary server as claimed in claim 44, further configured to:

encrypt each one of the one or more first requests with a second public key and sign each one of the one or more first requests with a first public key, before transmission to the second intermediary server; and

decrypt each one of the one or more first responses with a first private key after reception from the second intermediary server.

48. The first intermediary server as claimed in claim 37, further configured to:

receive the one or more second requests from a second intermediary server in the centralised financial system and transmit the one or more second requests to the first document store;

generate one or more second responses, each comprising the token, corresponding to the respective one or more second requests;

transmit the one or more second responses to the second intermediary server, via the messaging bus;

hash the one or more second requests and the one or more second responses to generate one or more second request hashes and one or more second response hashes, respectively; and

add the one or more second request hashes and the one or more second response hashes to the enriched data record in the blockchain.

49. The first intermediary server as claimed in claim 48, wherein the first intermediary server is further configured to:

encrypt each one of the one or more second responses with a second public key and sign the each one of the one or more second responses with a first public key, before transmission to the second intermediary server; and

decrypt each one of the one or more second requests with a first private key after reception from the second intermediary server.

50. The first intermediary server as claimed in claims 47 or 49, further configured to add the first public key into the blockchain.

51. A second intermediary server for use in a centralised financial system to facilitate processing of a financial transaction, operably connected to a network and a second document store, and configured to:

receive the token from the second digital device;

transmit the token to the second document store; and

send a second financial message comprising the token to a first intermediary server in the centralised financial system, indicative of making a payment to a first user.

52. A second intermediary server for use in a centralised financial system to facilitate processing of a financial transaction, operably connected to a network and a second document store, and configured to:

receive one or more first requests, each comprising a token, from a first intermediary server in the centralised financial system and transmit the one or more first requests and the token to the second document store;

generate the one or more first responses, each comprising the token, corresponding to the respective one or more first requests;

transmit the one or more first responses to the first intermediary server, via a messaging bus in the centralised financial system;

hash the one or more first requests and the one or more first responses to generate one or more first request hashes and one or more first response hashes, respectively; and

add the one or more first request hashes and the one or more first response hashes to the enriched data record in a blockchain being a distributed ledger.

53. The second intermediary server as claimed in claim 52, further configured to:

encrypt each one of the one or more first responses with a first public key and sign the each one of the one or more first responses with a second public key, before transmission to the first intermediary server; and

decrypt each one of the one or more first requests with a second private key after reception from the first intermediary server.

54. A second intermediary server for use in a centralised financial system to facilitate processing of a financial transaction, operably connected to a network and a second document store, and configured to:

transmit one or more second requests, each comprising a token, to a first intermediary server in the centralised financial system, via a messaging bus in the centralised financial system; and

receive one or more second responses from the first intermediary server and transmit the one or more second responses to the second document store.

55. The second intermediary server as claimed in claim 54, further configured to:

hash the one or more second responses to regenerate one or more second response hashes; and

verify the one or more second response hashes with a blockchain being a distributed ledger, using the token.

56. The second intermediary server as claimed in claim 54, further configured to:

encrypt each one of the one or more second requests with a first public key and sign each one of the one or more second requests with a second public key, before transmission to the first intermediary server; and

decrypt each one of the one or more second responses with a second private key after reception from the first intermediary server.

57. The second intermediary server as claimed in claims 53 or 56, further configured to add the second public key into the blockchain.

58. The second intermediary server as claimed in claim 54, wherein the one or more second responses comprise one or more first regulatory compliance documents pertaining to a first user.

PCT/AU2016/000279
Received 13/11/2017

Claims

1. A computer implemented method for processing a financial transaction, the method comprising the steps of:

transmitting one or more documents pertaining to the financial transaction, from a first intermediary server in a centralised financial system to a first document store;

generating an enriched data record from the one or more documents, at the first intermediary server, and adding the enriched data record into a blockchain being a distributed ledger, from the first intermediary sever;

requesting generation of a token corresponding to the financial transaction to identify the one or more documents, to a token server, from the first intermediary server, via a messaging bus in the centralised financial system;

generating the token at the token server and adding the token into the blockchain from the token server in association with the enriched data record;

transmitting the token to the first intermediary server from the token server, via the messaging bus; and

transmitting the token from the first intermediary server to the first document store in association with the one or more documents.

2. The computer implemented method as claimed in claim 1, further comprising the step of sending a first financial message comprising the token, from the first intermediary server to a second intermediary server in the centralised financial system, indicative of making a payment to a second user.

3. The computer implemented method as claimed in claim 1, further comprising the steps of:

implementing a smart contract at the token server; and

adding the smart contract into the blockchain, from the token server.

PCT/AU2016/000279
Received 13/11/2017

4. The computer implemented method as claimed in claim 1, further comprising the steps of:

transmitting the token from the first intermediary server to a first digital device available with a first user;

providing the token to a second user, by the first user;

providing the token to a second intermediary server in the centralised financial system, from the second digital device;

transmitting the token to a second document store, from the second intermediary server; and

sending a second financial message comprising the token, from the second intermediary server to the first intermediary server, indicative of making a payment to the first user.

5. The computer implemented method as claimed in claim 1, wherein the step of generating the enriched data record comprises:

extracting a plurality of attributes from the one or more documents, at the first intermediary server; and

combining the plurality of attributes to generate the enriched data record, at the first intermediary server.

6. The computer implemented method as claimed in claim 1, wherein the step of generating the enriched data record comprises:

extracting a plurality of attributes from the one or more documents, at the first intermediary server;

de-identifying the plurality of attributes to obtain a plurality of de-identified attributes, at the first intermediary server; and

combining the plurality of de-identified attributes to generate the enriched data record, at the first intermediary server.

7. The computer implemented method as claimed in claim 1, wherein the step of generating the enriched data record comprises:

extracting a plurality of attributes from the one or more documents, at the first intermediary server;

hashing the plurality of attributes to generate a plurality of respective hashes, at the first intermediary server; and

PCT/AU2016/000279
Received 13/11/2017

combining the plurality of hashes to generate the enriched data record, at the first intermediary server.

8. The computer implemented method as claimed in claim 1, further comprising the step of assigning a payment risk rating to the token.

9. The computer implemented method as claimed in claim 1, further comprising the steps of:

transmitting one or more first requests, each comprising the token, from the first intermediary server to ~~the~~ a second intermediary server in the centralised financial system, via the messaging bus;

receiving the one or more first requests at the second intermediary server and transmitting the one or more first requests and the token from the second intermediary server to a second document store;

generating one or more first responses, each comprising the token, corresponding to the respective one or more first requests, at the second intermediary server;

transmitting the one or more first responses from the second intermediary server to the first intermediary server, via the messaging bus;

hashing the one or more first requests and the one or more first responses at the second intermediary server to generate one or more first request hashes and one or more first response hashes, respectively;

adding the one or more first request hashes and the one or more first response hashes to the enriched data record in the blockchain, from the second intermediary server; and

receiving the one or more first responses at the first intermediary server and transmitting the one or more first responses to the first document store.

10. The computer implemented method as claimed in claim 9, further comprising the steps of:

hashing the one or more first responses at the first intermediary server to regenerate the one or more first response hashes; and

verifying the one or more first response hashes with the blockchain from the first intermediary server, using the token.

PCT/AU2016/000279
Received 13/11/2017

11. The computer implemented method as claimed in claim 9, wherein each one of the one or more first requests are:

encrypted with a second public key and signed with a first public key at the first intermediary server, before transmission to the second intermediary server; and

decrypted with a second private key at the second intermediary server after reception from the first intermediary server; and

wherein each one of the one or more first responses are:

encrypted with the first public key and signed with the second public key at the second intermediary server, before transmission to the first intermediary server; and

decrypted with a first private key at the first intermediary server after reception from the second intermediary server.

12. The computer implemented method as claimed in claim 9, wherein the one or more first responses comprise one or more second regulatory compliance documents pertaining to a second user.

13. The computer implemented method as claimed in claim 1, further comprising the steps of:

transmitting one or more second requests, each comprising the token, from ~~the~~ a second intermediary server in the centralised financial system to the first intermediary server, via the messaging bus;

receiving the one or more second requests at the first intermediary server and transmitting the one or more second requests from the first intermediary server to the first document store;

generating one or more second responses, each comprising the token, corresponding to the respective one or more second requests, at the first intermediary server;

transmitting the one or more second responses from the first intermediary server to the second intermediary server, via the messaging bus;

hashing the one or more second requests and the one or more second responses at the first intermediary server to generate one or more

PCT/AU2016/000279
Received 13/11/2017

second request hashes and one or more second response hashes, respectively;

adding the one or more second request hashes and the one or more second response hashes to the enriched data record in the blockchain, from the first intermediary server; and

receiving the one or more second responses at the second intermediary server and transmitting the one or more second responses to the second document store.

14. The computer implemented method as claimed in claim 13, further comprising the steps of:

hashing the one or more second responses at the second intermediary server to regenerate the one or more second response hashes; and

verifying the one or more second response hashes with the blockchain from the second intermediary server, using the token.

15. The computer implemented method as claimed in claim 13, wherein each one of the one or more second requests are:

encrypted with a first public key and signed with a second public key at the second intermediary server, before transmission to the first intermediary server; and

decrypted with a first private key at the first intermediary server after reception from the second intermediary server; and

wherein each one of the one or more second responses are:

encrypted with the second public key and signed with the first public key at the first intermediary server, before transmission to the second intermediary server; and

decrypted with a second private key at the second intermediary server after reception from the first intermediary server.

16. The computer implemented method as claimed in claim 11 or 15, further comprising the steps of adding the first public key from the first intermediary server into the blockchain and adding the second public key from the second intermediary server into the blockchain.

PCT/AU2016/000279
Received 13/11/2017

17. The computer implemented method as claimed in claim 13, wherein the one or more second responses comprise one or more first regulatory compliance documents pertaining to a first user.

18. A system for processing a financial transaction, the system comprising:

a first intermediary server in a centralised financial system, the first intermediary server being operably connected to a network and a first document store;

a token server operably connected to the network;

a messaging bus in the centralised financial system, the messaging bus being operably connected to the network; and

a blockchain operably connected to the network, the blockchain being a distributed ledger;

wherein the first intermediary server is configured to:

transmit one or more documents pertaining to the financial transaction, to the first document store;

generate an enriched data record from the one or more documents and add the enriched data record into the blockchain;

request generation of a token corresponding to the financial transaction to identify the one or more documents, to the token server, via the messaging bus; and

transmit the token to the first document store;

wherein the token server is configured to:

generate the token and add the token into the blockchain in association with the enriched data record; and

transmit the token to the first intermediary server, via the messaging bus.

19. The system as claimed in claim 18, further comprising a second intermediary server in the centralised financial system, operably connected to the network and a second document store;

wherein the first intermediary server is further configured to send a first financial message comprising the token, to the second intermediary server, indicative of making a payment to a second user.

PCT/AU2016/000279
Received 13/11/2017

20. The system as claimed in claim 18, wherein the token server is further configured to:

implement a smart contract; and

add the smart contract into the blockchain.

21. The system as claimed in claim 18, further comprising:

a first digital device operably connected to the network;

a second digital device operably connected to the network;

a second intermediary server in the centralised financial system, the second intermediary server being operably connected to the network and a second document store;

wherein the first intermediary server is further configured to:

transmit the token to the first digital device;

wherein the first digital device comprises a first memory and a first processor operably connected to the first memory, the first memory comprising a first computer program code, the first computer program code when executed by the first processor, instructs the first processor to:

receive the token from the first intermediary server;

provide the token to the second digital device;

wherein the second digital device comprises a second memory and a second processor operably connected to the second memory, the second memory comprising a second computer program code, the second computer program code when executed by the second processor, instructs the second processor to:

receive the token from the first digital device; and

provide the token to the second intermediary server; and

wherein the second intermediary server is configured to:

receive the token from the second digital device;

transmit the token to the second document store; and

send a second financial message comprising the token, to the first intermediary server, indicative of making a payment to a first user.

22. The system as claimed in claim 18, wherein for generation of the enriched data record, the first intermediary server is configured to:

extract a plurality of attributes from the one or more documents; and

combine the plurality of attributes to generate the enriched data record.

23. The system as claimed in claim 18, wherein for generation of the enriched data record, the first intermediary server is configured to:

extract a plurality of attributes from the one or more documents;

de-identify the plurality of attributes to obtain a plurality of de-identified attributes; and

combine the plurality of de-identified attributes to generate the enriched data record.

24. The system as claimed in claim 18, wherein for generation of the enriched data record, the first intermediary server is configured to:

extract a plurality of attributes from the one or more documents;

hash the plurality of attributes to generate a plurality of respective hashes; and

combine the plurality of hashes to generate the enriched data record.

25. The system as claimed in claim 18, wherein the first intermediary server is further configured to assign a payment risk rating to the token.

26. The system as claimed in claim 18, further comprising:

a second intermediary server in the centralised financial system, the second intermediary server being operably connected to the network and a second document store;

wherein the first intermediary server is configured to:

transmit one or more first requests, each comprising the token, to the second intermediary server, via the messaging bus; and

PCT/AU2016/000279
Received 13/11/2017

receive one or more first responses and transmit the one or more first responses to the first document store;

wherein the second intermediary server is configured to:

receive the one or more first requests from the first intermediary server and transmit the one or more first requests and the token to the second document store;

generate the one or more first responses, each comprising the token, corresponding to the respective one or more first requests;

transmit the one or more first responses to the first intermediary server, via the messaging bus;

hash the one or more first requests and the one or more first responses to generate one or more first request hashes and one or more first response hashes, respectively; and

add the one or more first request hashes and the one or more first response hashes to the enriched data record in the blockchain.

27. The system as claimed in claim 26, wherein the first intermediary server is further configured to:

hash the one or more first responses to regenerate the one or more first response hashes; and

verify the one or more first response hashes with the blockchain, using the token.

28. The system as claimed in claim 26, wherein the first intermediary server is further configured to:

encrypt each one of the one or more first requests with a second public key and sign each one of the one or more first requests with a first public key, before transmission to the second intermediary server; and

decrypt each one of the one or more first responses with a first private key after reception from the second intermediary server;

wherein the second intermediary server is further configured to:

encrypt the each one of the one or more first responses with the first public key and sign the each one of the one or more first

PCT/AU2016/000279
Received 13/11/2017

responses with the second public key, before transmission to the first intermediary server; and

decrypt the each one of the one or more first requests with a second private key after reception from the first intermediary server.

29. The system as claimed in claim 26, wherein the one or more first responses comprise one or more second regulatory compliance documents pertaining to a second user.

30. The system as claimed in claim 18, further comprising:

a second intermediary server in the centralised financial system, the second intermediary server being connected to the network and a second document store;

wherein the second intermediary server is configured to:

transmit one or more second requests, each comprising the token, to the first intermediary server, via the messaging bus;

receive one or more second responses and transmit the one or more second responses to the second document store;

wherein the first intermediary server is further configured to:

receive the one or more second requests and transmit the one or more second requests to the first document store;

generate the one or more second responses, each comprising the token, corresponding to the respective one or more second requests;

transmit the one or more second responses to the second intermediary server, via the messaging bus;

hash the one or more second requests and the one or more second responses to generate one or more second request hashes and one or more second response hashes, respectively; and

add the one or more second request hashes and the one or more second response hashes to the enriched data record in the blockchain.

31. The system as claimed in claim 30, wherein the second intermediary server is further configured to:

PCT/AU2016/000279
Received 13/11/2017

hash the one or more second responses to regenerate the one or more second response hashes; and

verify the one or more second response hashes with the blockchain, using the token.

32. The system as claimed in claim 30, wherein the second intermediary server is further configured to:

encrypt each one of the one or more second requests with a first public key and sign each one of the one or more second requests with a second public key, before transmission to the first intermediary server; and

decrypt each one of the one or more second responses with a second private key after reception from the first intermediary server;

wherein the first intermediary server is further configured to:

encrypt the each one of the one or more second responses with the second public key and sign the each one of the one or more second responses with the first public key, before transmission to the second intermediary server; and

decrypt the each one of the one or more second requests with a first private key after reception from the second intermediary server.

33. The system as claimed in claim 28 or 32, wherein the first intermediary server is further configured to add the first public key into the blockchain and the second intermediary server is further configured to add the second public key into the blockchain.

34. The system as claimed in claim 30, wherein the one or more second responses comprise one or more first regulatory compliance documents pertaining to a first user.

35. A token server for facilitating processing of a financial transaction, operably connected to a network and configured to generate a token, add the token into a blockchain <u>being a distributed ledger</u> and transmit the token to a first intermediary server <u>in a centralised financial system</u>, via a messaging bus <u>in the centralised financial system</u>.

PCT/AU2016/000279
Received 13/11/2017

36. The token server as claimed in claim 35, further configured to:

implement a smart contract; and

add the smart contract into the blockchain

37. A first intermediary server for use in a centralised financial system to facilitate~~ing~~ processing of a financial transaction, operably connected to a network and a first document store, and configured to:

transmit one or more documents pertaining to the financial transaction, to the first document store;

generate an enriched data record from the one or more documents and add the enriched data record into a blockchain being a distributed ledger;

request generation of a token corresponding to the financial transaction to identify the one or more documents, to a token server, via a messaging bus in the centralised financial system; and

transmit the token to the first document store.

38. The first intermediary server as claimed in claim 37, further configured to send a first financial message comprising the token, to a second intermediary server in the centralised financial system, indicative of making a payment to a second user.

39. The first intermediary server as claimed in claim 37, further configured to transmit the token to a first digital device.

40. The first intermediary server as claimed in claim 37, wherein for generation of the enriched data record, the first intermediary server is configured to:

extract a plurality of attributes from the one or more documents; and

combine the plurality of attributes to generate the enriched data record.

41. The first intermediary server as claimed in claim 37, wherein for generation of the enriched data record, the first intermediary server is configured:

PCT/AU2016/000279
Received 13/11/2017

extract a plurality of attributes from the one or more documents;

de-identify the plurality of attributes to obtain a plurality of de-identified attributes; and

combine the plurality of de-identified attributes to generate the enriched data record.

42. The first intermediary server as claimed in claim 37, wherein for generation of the enriched data record, the first intermediary server is configured to:

extract a plurality of attributes from the one or more documents;

hash the plurality of attributes to generate a plurality of respective hashes; and

combine the plurality of hashes to generate the enriched data record.

43. The first intermediary server as claimed in claim 37, further configured to assign a payment risk rating to the token.

44. The first intermediary server as claimed in claim 37, further configured to:

transmit one or more first requests, each comprising the token, to a second intermediary server in the centralised financial system, via the messaging bus; and

receive one or more first responses from the second intermediary server and transmit the one or more first responses to the first document store.

45. The first intermediary server as claimed in claim 44, wherein the one or more first responses comprise one or more second regulatory compliance documents pertaining to a second user.

46. The first intermediary server as claimed in claim 44, further configured to:

hash the one or more first responses to regenerate one or more first response hashes; and

verify the one or more first response hashes with the blockchain, using the token.

PCT/AU2016/000279
Received 13/11/2017

47. The first intermediary server as claimed in claim 44, further configured to:

encrypt each one of the one or more first requests with a second public key and sign each one of the one or more first requests with a first public key, before transmission to the second intermediary server; and

decrypt each one of the one or more first responses with a first private key after reception from the second intermediary server.

48. The first intermediary server as claimed in claim 37, further configured to:

receive the one or more second requests from a second intermediary server in the centralised financial system and transmit the one or more second requests to the first document store;

generate one or more second responses, each comprising the token, corresponding to the respective one or more second requests;

transmit the one or more second responses to the second intermediary server, via the messaging bus;

hash the one or more second requests and the one or more second responses to generate one or more second request hashes and one or more second response hashes, respectively; and

add the one or more second request hashes and the one or more second response hashes to the enriched data record in the blockchain.

49. The first intermediary server as claimed in claim 48, wherein the first intermediary server is further configured to:

encrypt each one of the one or more second responses with a second public key and sign the each one of the one or more second responses with a first public key, before transmission to the second intermediary server; and

decrypt each one of the one or more second requests with a first private key after reception from the second intermediary server.

50. The first intermediary server as claimed in claims 47 or 49, further configured to add the first public key into the blockchain.

PCT/AU2016/000279
Received 13/11/2017

51. A second intermediary server for use in a centralised financial system to facilitate~~ing~~ processing of a financial transaction, operably connected to a network and a second document store, and configured to:

receive the token from the second digital device;

transmit the token to the second document store; and

send a second financial message comprising the token to a first intermediary server in the centralised financial system, indicative of making a payment to a first user.

52. A second intermediary server for use in a centralised financial system to facilitate~~ing~~ processing of a financial transaction, operably connected to a network and a second document store, and configured to:

receive one or more first requests, each comprising a token, from a first intermediary server in the centralised financial system and transmit the one or more first requests and the token to the second document store;

generate the one or more first responses, each comprising the token, corresponding to the respective one or more first requests;

transmit the one or more first responses to the first intermediary server, via a messaging bus in the centralised financial system;

hash the one or more first requests and the one or more first responses to generate one or more first request hashes and one or more first response hashes, respectively; and

add the one or more first request hashes and the one or more first response hashes to the enriched data record in ~~the~~ a blockchain being a distributed ledger.

53. The second intermediary server as claimed in claim 52, further configured to:

encrypt each one of the one or more first responses with a first public key and sign the each one of the one or more first responses with a second public key, before transmission to the first intermediary server; and

decrypt each one of the one or more first requests with a second private key after reception from the first intermediary server.

PCT/AU2016/000279
Received 13/11/2017

54. A second intermediary server for use in a centralised financial system to facilitate~~ing~~ processing of a financial transaction, operably connected to a network and a second document store, and configured to:

transmit one or more second requests, each comprising a token, to a first intermediary server in the centralised financial system, via a messaging bus in the centralised financial system; and

receive one or more second responses from the first intermediary server and transmit the one or more second responses to the second document store.

55. The second intermediary server as claimed in claim 54, further configured to:

hash the one or more second responses to regenerate one or more second response hashes; and

verify the one or more second response hashes with ~~the~~ a blockchain being a distributed ledger, using the token.

56. The second intermediary server as claimed in claim 54, further configured to:

encrypt each one of the one or more second requests with a first public key and sign each one of the one or more second requests with a second public key, before transmission to the first intermediary server; and

decrypt each one of the one or more second responses with a second private key after reception from the first intermediary server.

57. The second intermediary server as claimed in claims 53 or 56, further configured to add the second public key into the blockchain.

58. The second intermediary server as claimed in claim 54, wherein the one or more second responses comprise one or more first regulatory compliance documents pertaining to a first user.

P01740WO1

PCT REQUEST

Print Out (Original in Electronic Form)

0	**For receiving Office use only**	
0-1	International Application No.	PCT/AU2016/000279
0-2	International Filing Date	12 August 2016 (12.08.2016)
0-3	Name of receiving Office and "PCT International Application"	**Australian Patent Office** **PCT INTERNATIONAL APPLICATION**

0-4	**Form PCT/RO/101 PCT Request**	
0-4-1	Prepared Using	PCT-SAFE Version 3.51.073.249 MT/FOP 20160401/0.20.5.24
0-5	**Petition** The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty	
0-6	**Receiving Office (specified by the applicant)**	Australian Patent Office (RO/AU)
0-7	**Applicant's or agent's file reference**	P01740WO1
I	**Title of Invention**	A COMPUTER IMPLEMENTED METHOD FOR PROCESSING A FINANCIAL TRANSACTION AND A SYSTEM THEREFOR
II	**Applicant**	
II-1	This person is	Applicant only
II-2	Applicant for	All designated States
II-4	Name	Identitii Pty Ltd
II-5	Address	Suite 1 Level 3 66-72 Reservoir St. Surry Hills, New South Wales 2010 Australia
II-6	State of nationality	AU
II-7	State of residence	AU
III-1	**Applicant and/or inventor**	
III-1-1	This person is	Inventor only
III-1-3	Inventor for	All designated States
III-1-4	Name (LAST, First)	ARMSTRONG, Nick
III-1-5	Address	Suite 1 Level 3 66-72 Reservoir St. Surry Hills, New South Wales 2010 Australia

P01740WO1

PCT REQUEST

Print Out (Original in Electronic Form)

III-2	**Applicant and/or inventor**	
III-2-1	This person is	Inventor only
III-2-3	Inventor for	All designated States
III-2-4	Name (LAST, First)	BUCKINGHAM, Ben
III-2-5	Address	Suite 1 Level 3 66-72 Reservoir St Surry Hills, New South Wales 2010 Australia
III-3	**Applicant and/or inventor**	
III-3-1	This person is	Inventor only
III-3-3	Inventor for	All designated States
III-3-4	Name (LAST, First)	FRIEDMAN, Daniel
III-3-5	Address	Suite 1 Level 3 66-72 Reservoir St. Surry Hills, New South Wales 2010 Australia
III-4	**Applicant and/or inventor**	
III-4-1	This person is	Inventor only
III-4-3	Inventor for	All designated States
III-4-4	Name (LAST, First)	SHEPHERD, Elliot
III-4-5	Address	Suite 1 Level 3 66-72 Reservoir St Surry Hills, New South Wales 2010 Australia
III-5	**Applicant and/or inventor**	
III-5-1	This person is	Inventor only
III-5-3	Inventor for	All designated States
III-5-4	Name (LAST, First)	KNIGHT, Eric
III-5-5	Address	Suite 1 Level 3 66-72 Reservoir St Surry Hills, New South Wales 2010 Australia

P01740WO1

PCT REQUEST

Print Out (Original in Electronic Form)

IV-1	**Agent or common representative; or address for correspondence**	
	The person identified below is hereby/ has been appointed to act on behalf of the applicant(s) before the competent International Authorities as:	Agent
IV-1-1	Name	BAXTER PATENT ATTORNEYS PTY LTD
IV-1-2	Address	Suite 2, Level 3A 1 Bligh St Sydney, New South Wales 2000 Australia
IV-1-3	Telephone No.	+61 02 9264 6716
IV-1-5	e-mail	mail@baxterip.com.au
IV-1-5(a)	E-mail authorization The receiving Office, the International Searching Authority, the International Bureau and the International Preliminary Examining Authority are authorized to use this e-mail address, if the Office or Authority so wishes, to send notifications issued in respect of this international application:	exclusively in electronic form (no paper notifications will be sent)
V	**DESIGNATIONS**	
V-1	**The filing of this request constitutes under Rule 4.9(a), the designation of all Contracting States bound by the PCT on the international filing date, for the grant of every kind of protection available and, where applicable, for the grant of both regional and national patents.**	
VI-1	**Priority claim of earlier national application**	
VI-1-1	Filing date	14 August 2015 (14.08.2015)
VI-1-2	Number	2015903292
VI-1-3	Country or Member of WTO	AU
VI-2	**Priority claim of earlier national application**	
VI-2-1	Filing date	27 January 2016 (27.01.2016)
VI-2-2	Number	2016900239
VI-2-3	Country or Member of WTO	AU
VI-3	**Priority claim of earlier national application**	
VI-3-1	Filing date	20 May 2016 (20.05.2016)
VI-3-2	Number	2016901924
VI-3-3	Country or Member of WTO	AU
VI-4	**Priority document request**	
	The receiving Office is requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) identified above as item(s):	VI-1 VI-2 VI-3

P01740WO1

PCT REQUEST

Print Out (Original in Electronic Form)

VI-5	**Incorporation by reference :** where an element of the international application referred to in Article 11(1)(iii)(d) or (e) or a part of the description, claims or drawings referred to in Rule 20.5(a) is not otherwise contained in this international application but is completely contained in an earlier application whose priority is claimed on the date on which one or more elements referred to in Article 11(1)(iii) were first received by the receiving Office, that element or part is, subject to confirmation under Rule 20.6, incorporated by reference in this international application for the purposes of Rule 20.6.		
VII-1	**International Searching Authority Chosen**	Australian Patent Office (ISA/AU)	
VIII	**Declarations**	Number of declarations	
VIII-1	Declaration as to the identity of the inventor	–	
VIII-2	Declaration as to the applicant's entitlement, as at the international filing date, to apply for and be granted a patent	–	
VIII-3	Declaration as to the applicant's entitlement, as at the international filing date, to claim the priority of the earlier application	–	
VIII-4	Declaration of inventorship (only for the purposes of the designation of the United States of America)	–	
VIII-5	Declaration as to non-prejudicial disclosures or exceptions to lack of novelty	–	
IX	**Check list**	Number of sheets	Electronic file(s) attached
IX-1	Request (including declaration sheets)	5	✓
IX-2	Description	75	✓
IX-3	Claims	16	✓
IX-4	Abstract	1	✓
IX-5	Drawings	23	✓
IX-7	TOTAL	120	
	Accompanying Items	Paper document(s) attached	Electronic file(s) attached
IX-8	Fee calculation sheet	–	✓
IX-20	**Figure of the drawings which should accompany the abstract**	1	
IX-21	**Language of filing of the international application**	English	

P01740WO1

PCT REQUEST

Print Out (Original in Electronic Form)

X-1	**Signature of applicant, agent or common representative**	(PKCS7 Digital Signature)
X-1-1	Name	BAXTER PATENT ATTORNEYS PTY LTD
X-1-2	Name of signatory	Christopher J. BAXTER
X-1-3	Capacity (if such capacity is not obvious from reading the request)	Patent Attorney

FOR RECEIVING OFFICE USE ONLY

10-1	**Date of actual receipt of the purported international application**	
10-2	**Drawings:**	
10-2-1	Received	
10-2-2	Not received	
10-3	**Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application**	
10-4	**Date of timely receipt of the required corrections under PCT Article 11(2)**	
10-5	**International Searching Authority**	ISA/AU
10-6	**Transmittal of search copy delayed until search fee is paid**	YES

FOR INTERNATIONAL BUREAU USE ONLY

11-1	**Date of receipt of the record copy by the International Bureau**	

Claims

1. A computer implemented method for processing a financial transaction, the method comprising the steps of:

transmitting one or more documents pertaining to the financial transaction, from a first intermediary server to a first document store;

generating an enriched data record from the one or more documents, at the first intermediary server, and adding the enriched data record into a blockchain, from the first intermediary sever;

requesting generation of a token corresponding to the financial transaction, to a token server, from the first intermediary server, via a messaging bus;

generating the token at the token server and adding the token into the blockchain from the token server;

transmitting the token to the first intermediary server from the token server, via the messaging bus; and

transmitting the token from the first intermediary server to the first document store.

2. The computer implemented method as claimed in claim 1, further comprising the step of sending a first financial message comprising the token, from the first intermediary server to a second intermediary server, indicative of making a payment to a second user.

3. The computer implemented method as claimed in claim 1, further comprising the steps of:

implementing a smart contract at the token server; and

adding the smart contract into the blockchain, from the token server.

4. The computer implemented method as claimed in claim 1, further comprising the steps of:

transmitting the token from the first intermediary server to a first digital device available with a first user;

providing the token to a second user, by the first user;

providing the token to a second intermediary server, from the second digital device;

transmitting the token to a second document store, from the second intermediary server; and

sending a second financial message comprising the token, from the second intermediary server to the first intermediary server, indicative of making a payment to the first user.

5. The computer implemented method as claimed in claim 1, wherein the step of generating the enriched data record comprises:

extracting a plurality of attributes from the one or more documents, at the first intermediary server; and

combining the plurality of attributes to generate the enriched data record, at the first intermediary server.

6. The computer implemented method as claimed in claim 1, wherein the step of generating the enriched data record comprises:

extracting a plurality of attributes from the one or more documents, at the first intermediary server;

de-identifying the plurality of attributes to obtain a plurality of de-identified attributes, at the first intermediary server; and

combining the plurality of de-identified attributes to generate the enriched data record, at the first intermediary server.

7. The computer implemented method as claimed in claim 1, wherein the step of generating the enriched data record comprises:

extracting a plurality of attributes from the one or more documents, at the first intermediary server;

hashing the plurality of attributes to generate a plurality of respective hashes, at the first intermediary server; and

combining the plurality of hashes to generate the enriched data record, at the first intermediary server.

8. The computer implemented method as claimed in claim 1, further comprising the step of assigning a payment risk rating to the token.

9. The computer implemented method as claimed in claim 1, further comprising the steps of:

transmitting one or more first requests, each comprising the token, from the first intermediary server to the second intermediary server, via the messaging bus;

receiving the one or more first requests at the second intermediary server and transmitting the one or more first requests and the token from the second intermediary server to a second document store;

generating one or more first responses, each comprising the token, corresponding to the respective one or more first requests, at the second intermediary server;

transmitting the one or more first responses from the second intermediary server to the first intermediary server, via the messaging bus;

hashing the one or more first requests and the one or more first responses at the second intermediary server to generate one or more first request hashes and one or more first response hashes, respectively;

adding the one or more first request hashes and the one or more first response hashes to the enriched data record in the blockchain, from the second intermediary server; and

receiving the one or more first responses at the first intermediary server and transmitting the one or more first responses to the first document store.

10. The computer implemented method as claimed in claim 9, further comprising the steps of:

hashing the one or more first responses at the first intermediary server to regenerate the one or more first response hashes; and

verifying the one or more first response hashes with the blockchain from the first intermediary server, using the token.

11. The computer implemented method as claimed in claim 9, wherein each one of the one or more first requests are:

encrypted with a second public key and signed with a first public key at the first intermediary server, before transmission to the second intermediary server; and

decrypted with a second private key at the second intermediary server after reception from the first intermediary server; and

wherein each one of the one or more first responses are:

encrypted with the first public key and signed with the second public key at the second intermediary server, before transmission to the first intermediary server; and

decrypted with a first private key at the first intermediary server after reception from the second intermediary server.

12. The computer implemented method as claimed in claim 9, wherein the one or more first responses comprise one or more second regulatory compliance documents pertaining to a second user.

13. The computer implemented method as claimed in claim 1, further comprising the steps of:

transmitting one or more second requests, each comprising the token, from the second intermediary server to the first intermediary server, via the messaging bus;

receiving the one or more second requests at the first intermediary server and transmitting the one or more second requests from the first intermediary server to the first document store;

generating one or more second responses, each comprising the token, corresponding to the respective one or more second requests, at the first intermediary server;

transmitting the one or more second responses from the first intermediary server to the second intermediary server, via the messaging bus;

hashing the one or more second requests and the one or more second responses at the first intermediary server to generate one or more second request hashes and one or more second response hashes, respectively;

adding the one or more second request hashes and the one or more second response hashes to the enriched data record in the blockchain, from the first intermediary server; and

receiving the one or more second responses at the second intermediary server and transmitting the one or more second responses to the second document store.

14. The computer implemented method as claimed in claim 13, further comprising the steps of:

hashing the one or more second responses at the second intermediary server to regenerate the one or more second response hashes; and

verifying the one or more second response hashes with the blockchain from the second intermediary server, using the token.

15. The computer implemented method as claimed in claim 13, wherein each one of the one or more second requests are:

encrypted with a first public key and signed with a second public key at the second intermediary server, before transmission to the first intermediary server; and

decrypted with a first private key at the first intermediary server after reception from the second intermediary server; and

wherein each one of the one or more second responses are:

encrypted with the second public key and signed with the first public key at the first intermediary server, before transmission to the second intermediary server; and

decrypted with a second private key at the second intermediary server after reception from the first intermediary server.

16. The computer implemented method as claimed in claim 11 or 15, further comprising the steps of adding the first public key from the first intermediary server into the blockchain and adding the second public key from the second intermediary server into the blockchain.

17. The computer implemented method as claimed in claim 13, wherein the one or more second responses comprise one or more first regulatory compliance documents pertaining to a first user.

18. A system for processing a financial transaction, the system comprising:

a first intermediary server operably connected to a network and a first document store;

a token server operably connected to the network;

a messaging bus operably connected to the network; and

a blockchain operably connected to the network;

wherein the first intermediary server is configured to:

transmit one or more documents pertaining to the financial transaction, to the first document store;

generate an enriched data record from the one or more documents and add the enriched data record into the blockchain;

request generation of a token corresponding to the financial transaction, to the token server, via the messaging bus; and

transmit the token to the first document store;

wherein the token server is configured to:

generate the token and add the token into the blockchain; and

transmit the token to the first intermediary server, via the messaging bus.

19. The system as claimed in claim 18, further comprising a second intermediary server operably connected to the network and a second document store;

wherein the first intermediary server is further configured to send a first financial message comprising the token, to the second intermediary server, indicative of making a payment to a second user.

20. The system as claimed in claim 18, wherein the token server is further configured to:

implement a smart contract; and

add the smart contract into the blockchain.

21. The system as claimed in claim 18, further comprising:

a first digital device operably connected to the network;

a second digital device operably connected to the network;

a second intermediary server operably connected to the network and a second document store;

wherein the first intermediary server is further configured to:

transmit the token to the first digital device;

wherein the first digital device comprises a first memory and a first processor operably connected to the first memory, the first memory comprising a first computer program code, the first computer program code when executed by the first processor, instructs the first processor to:

receive the token from the first intermediary server;

provide the token to the second digital device;

wherein the second digital device comprises a second memory and a second processor operably connected to the second memory, the second memory comprising a second computer program code, the second computer program code when executed by the second processor, instructs the second processor to:

receive the token from the first digital device; and

provide the token to the second intermediary server; and

wherein the second intermediary server is configured to:

receive the token from the second digital device;

transmit the token to the second document store; and

send a second financial message comprising the token, to the first intermediary server, indicative of making a payment to a first user.

22. The system as claimed in claim 18, wherein for generation of the enriched data record, the first intermediary server is configured to:

extract a plurality of attributes from the one or more documents; and

combine the plurality of attributes to generate the enriched data record.

23. The system as claimed in claim 18, wherein for generation of the enriched data record, the first intermediary server is configured to:

extract a plurality of attributes from the one or more documents;

de-identify the plurality of attributes to obtain a plurality of de-identified attributes; and

combine the plurality of de-identified attributes to generate the enriched data record.

24. The system as claimed in claim 18, wherein for generation of the enriched data record, the first intermediary server is configured to:

extract a plurality of attributes from the one or more documents;

hash the plurality of attributes to generate a plurality of respective hashes; and

combine the plurality of hashes to generate the enriched data record.

25. The system as claimed in claim 18, wherein the first intermediary server is further configured to assign a payment risk rating to the token.

26. The system as claimed in claim 18, further comprising:

a second intermediary server operably connected to the network and a second document store;

wherein the first intermediary server is configured to:

transmit one or more first requests, each comprising the token, to the second intermediary server, via the messaging bus; and

receive one or more first responses and transmit the one or more first responses to the first document store;

wherein the second intermediary server is configured to:

receive the one or more first requests from the first intermediary server and transmit the one or more first requests and the token to the second document store;

generate the one or more first responses, each comprising the token, corresponding to the respective one or more first requests;

transmit the one or more first responses to the first intermediary server, via the messaging bus;

hash the one or more first requests and the one or more first responses to generate one or more first request hashes and one or more first response hashes, respectively; and

add the one or more first request hashes and the one or more first response hashes to the enriched data record in the blockchain.

27. The system as claimed in claim 26, wherein the first intermediary server is further configured to:

hash the one or more first responses to regenerate the one or more first response hashes; and

verify the one or more first response hashes with the blockchain, using the token.

28. The system as claimed in claim 26, wherein the first intermediary server is further configured to:

encrypt each one of the one or more first requests with a second public key and sign each one of the one or more first requests with a first public key, before transmission to the second intermediary server; and

decrypt each one of the one or more first responses with a first private key after reception from the second intermediary server;

wherein the second intermediary server is further configured to:

encrypt the each one of the one or more first responses with the first public key and sign the each one of the one or more first responses with the second public key, before transmission to the first intermediary server; and

decrypt the each one of the one or more first requests with a second private key after reception from the first intermediary server.

29. The system as claimed in claim 26, wherein the one or more first responses comprise one or more second regulatory compliance documents pertaining to a second user.

30. The system as claimed in claim 18, further comprising:

a second intermediary server connected to the network and a second document store;

wherein the second intermediary server is configured to:

transmit one or more second requests, each comprising the token, to the first intermediary server, via the messaging bus;

receive one or more second responses and transmit the one or more second responses to the second document store;

wherein the first intermediary server is further configured to:

receive the one or more second requests and transmit the one or more second requests to the first document store;

generate the one or more second responses, each comprising the token, corresponding to the respective one or more second requests;

transmit the one or more second responses to the second intermediary server, via the messaging bus;

hash the one or more second requests and the one or more second responses to generate one or more second request hashes and one or more second response hashes, respectively; and

add the one or more second request hashes and the one or more second response hashes to the enriched data record in the blockchain.

31. The system as claimed in claim 30, wherein the second intermediary server is further configured to:

hash the one or more second responses to regenerate the one or more second response hashes; and

verify the one or more second response hashes with the blockchain, using the token.

32. The system as claimed in claim 30, wherein the second intermediary server is further configured to:

encrypt each one of the one or more second requests with a first public key and sign each one of the one or more second requests with a second public key, before transmission to the first intermediary server; and

decrypt each one of the one or more second responses with a second private key after reception from the first intermediary server;

wherein the first intermediary server is further configured to:

encrypt the each one of the one or more second responses with the second public key and sign the each one of the one or more second responses with the first public key, before transmission to the second intermediary server; and

decrypt the each one of the one or more second requests with a first private key after reception from the second intermediary server.

33. The system as claimed in claim 28 or 32, wherein the first intermediary server is further configured to add the first public key into the blockchain and the second intermediary server is further configured to add the second public key into the blockchain.

34. The system as claimed in claim 30, wherein the one or more second responses comprise one or more first regulatory compliance documents pertaining to a first user.

35. A token server for facilitating processing of a financial transaction, operably connected to a network and configured to generate a token, add the token into a blockchain and transmit the token to a first intermediary server, via a messaging bus.

36. The token server as claimed in claim 35, further configured to:

implement a smart contract; and

add the smart contract into the blockchain

37. A first intermediary server for facilitating processing of a financial transaction, operably connected to a network and a first document store, and configured to:

transmit one or more documents pertaining to the financial transaction, to the first document store;

generate an enriched data record from the one or more documents and add the enriched data record into a blockchain;

request generation of a token corresponding to the financial transaction, to a token server, via a messaging bus; and

transmit the token to the first document store.

38. The first intermediary server as claimed in claim 37, further configured to send a first financial message comprising the token, to a second intermediary server, indicative of making a payment to a second user.

39. The first intermediary server as claimed in claim 37, further configured to transmit the token to a first digital device.

40. The first intermediary server as claimed in claim 37, wherein for generation of the enriched data record, the first intermediary server is configured to:

extract a plurality of attributes from the one or more documents; and

combine the plurality of attributes to generate the enriched data record.

41. The first intermediary server as claimed in claim 37, wherein for generation of the enriched data record, the first intermediary server is configured:

extract a plurality of attributes from the one or more documents;

de-identify the plurality of attributes to obtain a plurality of de-identified attributes; and

combine the plurality of de-identified attributes to generate the enriched data record.

42. The first intermediary server as claimed in claim 37, wherein for generation of the enriched data record, the first intermediary server is configured to:

extract a plurality of attributes from the one or more documents;

hash the plurality of attributes to generate a plurality of respective hashes; and

combine the plurality of hashes to generate the enriched data record.

43. The first intermediary server as claimed in claim 37, further configured to assign a payment risk rating to the token.

44. The first intermediary server as claimed in claim 37, further configured to:

transmit one or more first requests, each comprising the token, to a second intermediary server, via the messaging bus; and

receive one or more first responses from the second intermediary server and transmit the one or more first responses to the first document store.

45. The first intermediary server as claimed in claim 44, wherein the one or more first responses comprise one or more second regulatory compliance documents pertaining to a second user.

46. The first intermediary server as claimed in claim 44, further configured to:

hash the one or more first responses to regenerate one or more first response hashes; and

verify the one or more first response hashes with the blockchain, using the token.

47. The first intermediary server as claimed in claim 44, further configured to:

encrypt each one of the one or more first requests with a second public key and sign each one of the one or more first requests with a first public key, before transmission to the second intermediary server; and

decrypt each one of the one or more first responses with a first private key after reception from the second intermediary server.

48. The first intermediary server as claimed in claim 37, further configured to:

receive the one or more second requests from a second intermediary server and transmit the one or more second requests to the first document store;

generate one or more second responses, each comprising the token, corresponding to the respective one or more second requests;

transmit the one or more second responses to the second intermediary server, via the messaging bus;

hash the one or more second requests and the one or more second responses to generate one or more second request hashes and one or more second response hashes, respectively; and

add the one or more second request hashes and the one or more second response hashes to the enriched data record in the blockchain.

49. The first intermediary server as claimed in claim 48, wherein the first intermediary server is further configured to:

encrypt each one of the one or more second responses with a second public key and sign the each one of the one or more second responses with a first public key, before transmission to the second intermediary server; and

decrypt each one of the one or more second requests with a first private key after reception from the second intermediary server.

50. The first intermediary server as claimed in claims 47 or 49, further configured to add the first public key into the blockchain.

51. A second intermediary server for facilitating processing of a financial transaction, operably connected to a network and a second document store, and configured to:

receive the token from the second digital device;

transmit the token to the second document store; and

send a second financial message comprising the token to a first intermediary server, indicative of making a payment to a first user.

52. A second intermediary server for facilitating processing of a financial transaction, operably connected to a network and a second document store, and configured to:

receive one or more first requests, each comprising a token, from a first intermediary server and transmit the one or more first requests and the token to the second document store;

generate the one or more first responses, each comprising the token, corresponding to the respective one or more first requests;

transmit the one or more first responses to the first intermediary server, via a messaging bus;

hash the one or more first requests and the one or more first responses to generate one or more first request hashes and one or more first response hashes, respectively; and

add the one or more first request hashes and the one or more first response hashes to the enriched data record in the blockchain.

53. The second intermediary server as claimed in claim 52, further configured to:

encrypt each one of the one or more first responses with a first public key and sign the each one of the one or more first responses with a second public key, before transmission to the first intermediary server; and

decrypt each one of the one or more first requests with a second private key after reception from the first intermediary server.

54. A second intermediary server for facilitating processing of a financial transaction, operably connected to a network and a second document store, and configured to:

transmit one or more second requests, each comprising a token, to a first intermediary server, via a messaging bus; and

receive one or more second responses from the first intermediary server and transmit the one or more second responses to the second document store.

55. The second intermediary server as claimed in claim 54, further configured to:

hash the one or more second responses to regenerate one or more second response hashes; and

verify the one or more second response hashes with the blockchain, using the token.

56. The second intermediary server as claimed in claim 54, further configured to:

encrypt each one of the one or more second requests with a first public key and sign each one of the one or more second requests with a second public key, before transmission to the first intermediary server; and

decrypt each one of the one or more second responses with a second private key after reception from the first intermediary server.

57. The second intermediary server as claimed in claims 53 or 56, further configured to add the second public key into the blockchain.

58. The second intermediary server as claimed in claim 54, wherein the one or more second responses comprise one or more first regulatory compliance documents pertaining to a first user.