PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY
(Chapter I of the Patent Cooperation Treaty)

(PCT Rule 44*bis*)

Applicant's or agent's file reference 226.P100.PCT	**FOR FURTHER ACTION**	See item 4 below
International application No. PCT/US2015/029196	International filing date *(day/month/year)* 05 May 2015 (05.05.2015)	Priority date *(day/month/year)* 09 May 2014 (09.05.2014)
International Patent Classification (8th edition unless older edition indicated) See relevant information in Form PCT/ISA/237		
Applicant VERITASEUM, INC.		

1. This international preliminary report on patentability (Chapter I) is issued by the International Bureau on behalf of the International Searching Authority under Rule 44 *bis*.1(a).

2. This REPORT consists of a total of 9 sheets, including this cover sheet.

   In the attached sheets, any reference to the written opinion of the International Searching Authority should be read as a reference to the international preliminary report on patentability (Chapter I) instead.

3. This report contains indications relating to the following items:

☒	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
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or 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

4. The International Bureau will communicate this report to designated Offices in accordance with Rules 44*bis*.3(c) and 93*bis*.1 but not, except where the applicant makes an express request under Article 23(2), before the expiration of 30 months from the priority date (Rule 44*bis* .2).

	Date of issuance of this report 15 November 2016 (15.11.2016)
The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. +41 22 338 82 70	Authorized officer Kihwan Moon e-mail: pt01.pct@wipo.int

Form PCT/IB/373 (January 2004)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To: JOHN E. NIELSEN
SENTINEL IP, PC
484 WASHINGTON ST
SUITE B-345
MONTEREY, CA 93940

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	07 AUG 2015
Applicant's or agent's file reference 226.P100.PCT	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US 15/29196	05 May 2015 (05.05.2015)	09 May 2014 (09.05.2014)

International Patent Classification (IPC) or both national classification and IPC
IPC(8) - H04L 29/06 (2015.01)
CPC - H04L9/00

Applicant VERITASEUM, INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ 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
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or 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

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1 *bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA/US	Date of completion of this opinion	Authorized officer:
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300	14 July 2015 (14.07.2015)	Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/237 (cover sheet) (January 2015)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 15/29196

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion 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 (Rules 12.3(a) and 23.1(b)).

2. [ ] This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a)).

3. [ ] With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing:
   - a. [ ] forming part of the international application as filed:
     - [ ] in the form of an Annex C/ST.25 text file.
     - [ ] on paper or in the form of an image file.
   - b. [ ] furnished together with the international application under PCT Rule 13*ter*.1(a) for the purposes of international search only in the form of an Annex C/ST.25 text file.
   - c. [ ] furnished subsequent to the international filing date for the purposes of international search only:
     - [ ] in the form of an Annex C/ST.25 text file (Rule 13*ter*.1(a)).
     - [ ] on paper or in the form of an image file (Rule 13*ter*.1(b) and Administrative Instructions, Section 713).

4. [ ] In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that forming part of the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 15/29196

Box No. V **Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	2, 12-30	YES
	Claims	1, 3-11	NO
Inventive step (IS)	Claims	None	YES
	Claims	1-30	NO
Industrial applicability (IA)	Claims	1-30	YES
	Claims	None	NO

2. Citations and explanations:

Claims 1 and 3-11 lack novelty under PCT Article 33(2) as being anticipated by US 2003/0070080 A1 (Rosen).

As to claim 1, Rosen teaches a device for facilitating a value transfer between a first party utilizing a first client and a second party utilizing a second client via a transfer mechanism (para [0026], [0149]-[0151], [0161], Fig. 56 - "Pay/Exchange application 35 supervises the sending and receiving of electronic notes 11 between Transaction money modules"), the device comprising: a. a first memory comprising a transaction record sector and a first key pair sector for storing a first asymmetric key pair, the first asymmetric key pair comprising a first private key and a first public key (para [0162], [0685]-[0688], claim 1, claim 2, claim 13 - "Tran Log Mgr. application 36 provides the management and overseeing of a log that records completed transactions undertaken by the money module"; "Each primary trusted server 210 has its own public key and corresponding private key"); b. a first network interface for receiving terms (para [0231]-[0234] - "communication layer will carry transaction requests (e.g., deposits, withdrawals), packets of notes 11 and new certificates securely across the Network"), the terms comprising: i a first principal amount (para [0165] - "the amount of transfer"); and ii. a reference to a first data source (para [0159], [1297] - "accesses to the Transaction money module's 4 stored contents"; "account reference files"); and c. a first computer processor coupled to the first memory and the first network interface (para [0117], [0143], [0673] - "processor"), the first computer processor configured to: i retrieve a value from the first data source (para [0149], [0677] - "information retrieval"); ii. read the first private key from the first key pair sector (para [0504], claim 13 - "generating a private key retained in said memory"); iii. compute a first cryptographic signature from the first private key (para [0660], [0662], [0702] - "private key used for encrypting and for creating digital signature"); iv. create an inchoate disbursement transaction record comprising: A. a commit input for receiving a commit amount from a commit transaction (para [0157], [0546], [1941] - "session manager 31 to control and commit (i.e., finalize) or abort a transaction session"); and B. the first cryptographic signature (para [1946] - "security server 1184 digitally signs the new (or updated) profile (step 1846). The security server 1184 then sends the signed profile to the money module 1186 (step 1848). Finally, the money module to security server transaction commits (step 1850) and the security server to CSM transaction commits"); and v. publish the inchoate disbursement transaction record to at least one of the first client and the second client (para [0142]-[0143], [0588]-[0591], Fig. 3, Fig. 7 - "Pay/Exchange A 35 sends a message disclosing the amount of the transfer to Bob's Transaction money module 4 (Step 828), using the process disclosed in Steps 2-8. See FIG. 36A. From there, To Subscriber B 33 prompts the owner to verify that the amount to be transferred will be accepted"); where the first client comprises: a. a second memory comprising a second key pair sector for storing a second asymmetric key pair, the second asymmetric key pair comprising a second private key and a second public key (para [0142]-[0143], [0159], [0749], claim 91 - "Security Manager A requests Public Key A to generate a new public and private key pair"); b. a second network interface (para [0666] - "Communications function 128 sets up the connection between two transaction devices 122, or connects a transaction device to a network for indirect connection to another transaction device or a trusted server"); and c. a second computer processor coupled to the second memory and the second network interface, the second computer processor configured to read the second private key from the second key pair sector (para [0630], [0664], [0749], Fig. 52 - "trusted agent's public and private key pair are used in establishing a session between trusted agents 120 or between a trusted agent 120 and a trusted server"); and where the second client comprises; a. a third memory comprising a third key pair sector for storing a third asymmetric key pair, the third asymmetric key pair comprising a third private key and a third public key (para [1660]-[1663], Fig. 57A - "Each primary trusted server 210 has its own public key and corresponding private key"; "trusted server 200 requests the trusted agent 120 to generate a public and private key pair"); b. a third network interface (para [0670] - "Message Manager 134 routes inter-host messages (i.e., messages between transaction devices) and messages among the host processor 124, the trusted agent 120 and the money module"); and c. a third computer processor coupled to the third memory and the third network interface, the third computer processor configured to read the third private key from the third key pair sector (para [0664], [1660]-[1663], Fig. 56 - "trusted server 200 requests the trusted agent 120 to generate a public and private key pair").

As to claim 3, Rosen further teaches a device where: a. the first computer processor is further configured to compute a disbursement amount by applying a disbursement function to: i. the first principal amount; and ii. the value from the first data source; and b. the inchoate disbursement transaction record further comprises a disbursement output comprising the disbursement amount (para [0157]-[0174]).

As to claim 4, Rosen further teaches a device where the first computer processor is further configured to: a. compute a second cryptographic signature from the first private key; b. create an inchoate refund transaction record comprising: i. a commit input for receiving the commit amount from the commit transaction; ii. a refund output comprising a refund amount; iii. the second cryptographic signature; and iv. a lock time; and c. publish the inchoate refund transaction record to at least one of the first client or the second client (para [0157]-[0174], [0176]-[0179], [0251], [0300], [0806]-[0807], [0845]).

(See Continuation Box)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 15/29196

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:
Box V.2. Citations and explanations:

As to claim 5, Rosen further teaches a device where: a. the first key pair sector further stores a fourth asymmetric key pair, the fourth asymmetric key pair comprising a fourth private key and a fourth public key; and b. the first computer processor is further configured to: i. read the fourth private key from the first key pair sector; ii. compute a second cryptographic signature from the fourth private key; iii. create a commit transaction record, the commit transaction record comprising: A a first principal input for receiving the first principal amount from a first principal transaction; B. a commit output comprising the commit amount; C. the second cryptographic signature; and iv. create the commit transaction by submitting the commit transaction record to the transfer mechanism (para [0177], [0193], [0546], [0662], [0791]-[0802], [1723], claim 1, claim 2, claim 13).

As to claim 6, Rosen further teaches a device where the first asymmetric key pair consists of the fourth asymmetric key pair, the first private key consists of the fourth private key, and the first public key consists of the fourth public key (para [0193], [0683]-[0688], [0854], Fig. 56, claim 13 - key pairs may be created as needed).

As to claim 7, Rosen further teaches a device where: a. the terms further comprise: i. a second principal amount; and ii. an expiration timestamp; b. the first computer processor is further configured to compute the one or more disbursement amounts by applying a disbursement function to: i. the value from the first data source; and at least one of: A. the first principal amount; and B. the second principal amount; and c. the inchoate disbursement transaction record further comprises one or more disbursement outputs comprising the disbursement amounts (para [0157]-[0174], [0176]-[0179], [0535], [0798]-[0802]).

As to claim 8, Rosen further teaches a device where: a. the terms further comprise: i. a reference to a second data source; b. the first computer processor is further configured to compute the one or more disbursement amounts by applying the disbursement function to: i. the value from the first data source; ii. the value from the second data source; iii. the first principal amount; and iv. the second principal amount (para [0157]-[0174], [0176]-[0179], [0184], [0279], [0284]).

As to claim 9, Rosen further teaches a device where: a. the reference to the first data source comprises at least one of a reference to a base instrument and a reference to a quote instrument; and b. the first computer processor is further configured to compute the disbursement amounts on or after the expiration timestamp (para [0118], [0180], [0278], [0284], [0535]-[0540], [0628] - "subscriber may be able to select information on the total amount of the electronic notes 11 stored, the monetary unit of the notes 11, the type of electronic notes 11, i.e., currency or credit, and the denomination of each note").

As to claim 10, Rosen further teaches a device where the first computer processor is further configured to: a. compute a second cryptographic signature from the first private key; b. create an inchoate refund transaction record comprising: i. a commit input for receiving the commit amount from the commit transaction; ii. one or more refund outputs comprising one or more refund amounts; iii. the second cryptographic signature; and iv. a lock time; and c. publish the inchoate refund transaction record to at least one of the first client and the second client (para [0157]-[0174], [0176]-[0179], [0251], [0300], [0806]-[0807], [0845]).

As to claim 11, Rosen further teaches a device where: a. the first key pair sector further stores a fourth asymmetric key pair, the fourth asymmetric key pair comprising a fourth private key and a fourth public key; and b. the first computer processor is further configured to: i. read the fourth private key from the first key pair sector; ii. compute a second cryptographic signature from the fourth private key; iii. create a commit transaction record comprising: A. a first principal input for receiving the first principal amount from a first principal transaction; B. a second principal input for receiving the second principal amount from a second principal transaction; C. a commit output comprising a commit amount; and D. the second cryptographic signature; and iv. create the commit transaction by submitting the commit transaction record to the transfer mechanism (para [0177], [0193], [0255]-[0267], [0546], [0662], [0791]-[0802], [1723], claim 1, claim 2, claim 13).

Claims 2 and 12-30 lack an inventive step under PCT Article 33(3) as being obvious over Rosen in view of US 2013/0166455 A1 (Feigelson).

As to claim 2, Rosen further teaches a device where the transfer mechanism comprises a digital currency (para [0118] - "Electronic notes 11, the media for transferring electronic money"), but does not explicitly teach a decentralized digital currency. However, Feigelson does teach a decentralized digital currency (para [0050]-[0051] - "currency on the Bitcoin ecurrency network"). It would have been obvious to one of ordinary skill in the art to utilize a decentralized digital currency as taught by Feigelson in order to provide a monetary system using electronic media to exchange economic value securely and reliably as taught by Rosen capable of improved transaction security and less reliance on a central currency issuer.

(See Next Continuation Box)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 15/29196

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:
Box V.2. Citations and explanations:

As to claim 12, Rosen teaches a system for facilitating a value transfer between a first party utilizing a first client and a second party utilizing a second client via a transfer mechanism (para [0149]-[0151], [0161], Fig. 56), the transfer mechanism comprising a digital currency (para [0118]), the system comprising a facilitator, the first client, and the second client (para [0026] - "a plurality of transaction devices that are used by subscribers for storing electronic money, for performing money transactions with the on-line systems of the participating banks or for exchanging electronic money with other like transaction devices in off-line transactions"; "process handling and interfacing the transaction devices"); a. the facilitator comprising: i. a first memory comprising a transaction record sector and a first key pair sector for storing a first asymmetric key pair, the first asymmetric key pair comprising a first private key and a first public key (para [0162], [0685]-[0688], claim 1, claim 2, claim 13); ii. a first network interface for receiving terms (para [0231]-[0234]), the terms comprising: A. a first principal amount (para [0165]); and B. a reference to a first data source (para [0159], [1297]); and iii. a first computer processor coupled to the first memory and the first network interface (para [0117], [0143], [0673]), the first computer processor configured to: A. retrieve a value from the first data source (para [0149], [0677]); B. read the first private key from the first key pair sector (para [0504], claim 13); C. compute a first cryptographic signature from the first private key (para [0660], [0662], [0702]); D. create an inchoate disbursement transaction record comprising: I. a commit input for receiving a commit amount from a commit transaction (para [0157], [0546], [1941]); and II. the first cryptographic signature (para [1946]); and E. publish the inchoate disbursement transaction record to at least one of the first client and the second client (para [0142]-[0143], [0588]-[0591], Fig. 3, Fig. 7); b. the first client comprising: i. a second memory comprising a second key pair sector for storing a second asymmetric key pair, the second asymmetric key pair comprising a second private key and a second public key (para [0142]-[0143], [0159], [0749], claim 91); ii. a second network interface (para [0666]); and iii. a second computer processor coupled to the second memory and the second network interface, the second computer processor configured to read the second private key from the second key pair sector (para [0630], [0664], [0749], Fig. 52); and c. the second client comprising: i. a third memory comprising a third key pair sector for storing a third asymmetric key pair, the third asymmetric key pair comprising a third private key and a third public key (para [1660]-[1663], Fig. 57A); ii. a third network interface (para [0670]); and iii. a third computer processor coupled to the third memory and the third network interface, the third computer processor configured to read the third private key from the third key pair sector (para [0664], [1660]-[1663], Fig. 56), but does not explicitly teach a decentralized digital currency. However, Feigelson does teach a decentralized digital currency (para [0050]-[0051] - "currency on the Bitcoin ecurrency network"). It would have been obvious to one of ordinary skill in the art to utilize a decentralized digital currency as taught by Feigelson in order to provide a monetary system using electronic media to exchange economic value securely and reliably as taught by Rosen capable of improved transaction security and less reliance on a central currency issuer.

As to claim 13, Rosen further teaches a system where: a. the first computer processor consists of the second computer processor; b. the first memory consists of the second memory; and c. the first network interface consists of the second network interface (para [0143]-[0147], [0157]).

As to claim 14, Rosen further teaches a system where: a. the first computer processor is further configured compute a disbursement amount by applying a disbursement function to: i. the first principal amount; and ii. the value from the first data source; b. the inchoate disbursement transaction record further comprises a disbursement output comprising the disbursement amount; and c. the second computer processor is further configured to: i. read the inchoate disbursement transaction; ii. compute a second cryptographic signature from the second private key; iii. create a complete disbursement transaction record comprising: A. the commit input; B. the disbursement output; C. the first cryptographic signature; and D. the second cryptographic signature; and iv. create a disbursement transaction by submitting the complete disbursement transaction record to the transfer mechanism (para [0157]-[0174], [0177], [0193], [0288], [0504], [0546], [0662], [0791]-[0802], claim 1, claim 2, claim 13).

As to claim 15, Rosen further teaches a system where the first computer processor is further configured to: a. compute a second cryptographic signature from the first private key; b. create an inchoate refund transaction record comprising: i. a commit input for receiving the commit amount from the commit transaction; ii. a refund output comprising a refund amount; and iii. the second cryptographic signature; and c. publish the inchoate refund transaction record to at least one of the first client and the second client (para [0157]-[0174], [0176]-[0179], [0251], [0300], [0806]-[0807], [0845]).

As to claim 16, Rosen further teaches a system where: a. the first key pair sector further stores a fourth asymmetric key pair, the fourth asymmetric key pair comprising a fourth private key and a fourth public key; b. the first computer processor is further configured to: i. compute a disbursement amount by applying a disbursement function to: A. the first principal amount; and B. the value from the first data source; ii. read the fourth private key from the first key pair sector; iii. compute a second cryptographic signature from the fourth private key; iv. create a commit transaction record comprising: A. a first principal input for receiving the first principal amount from a first principal transaction; B. a commit output comprising the commit amount; and C. the second cryptographic signature; and v. create the commit transaction by submitting the commit transaction record to the transfer mechanism; and c. the inchoate disbursement transaction record further comprises a disbursement output comprising the disbursement amount (para [0157]-[0174], [0177], [0193], [0546], [0662], [0791]-[0802], claim 1, claim 2, claim 13).

As to claim 17, Rosen further teaches a system where the second computer processor is configured to: a. compute a third cryptographic signature from the second private key; b. create a first principal transaction record comprising: i. a first principal output comprising the first principal amount; and ii. the third cryptographic signature; and c. create the first principal transaction by submitting the first principal transaction record to the transfer mechanism (para [0157]-[0174], [0176]-[0179], [0300], [0791]-[0802]).

(See Next Continuation Box)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No. PCT/US 15/29196

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**

Continuation of:
Box V.2. Citations and explanations:

As to claim 18, Rosen further teaches a system where: a. the terms further comprise: i. a second principal amount; and ii. an expiration timestamp; b. the first computer processor is further configured compute one or more disbursement amounts by applying a disbursement function to: i. the value from the first data source; and at least one of: A. the first principal amount; and B. the second principal amount; c. the inchoate disbursement transaction record further comprises one or more disbursement outputs comprising the disbursement amounts; and d. the second computer processor is further configured to: i. read the inchoate disbursement transaction; ii. compute a second cryptographic signature from the second private key; iii. create a complete disbursement transaction record comprising: A. the commit input; B. the disbursement outputs; C. the first cryptographic signature; and D. the second cryptographic signature; and iv. create a disbursement transaction by submitting the complete disbursement transaction record to the transfer mechanism (para [0157]-[0174], [0176]-[0179], [0288], [0504], [0535], [0546], [0791]-[0802]).

As to claim 19, Rosen further teaches a system where: a. the terms further comprise: i. a reference to a second data source; b. the first computer processor is further configured to compute the one or more disbursement amounts by applying the disbursement function to: i. the value from the first data source; ii. the value from the second data source; iii. the first principal amount; and iv. the second principal amount (para [0157]-[0174], [0176]-[0179], [0184], [0279], [0284]).

As to claim 20, Rosen further teaches a system where: a. the reference to the first data source comprises at least one of a reference to a base instrument and a reference to a quote instrument; and b. the first computer processor is further configured to compute the disbursement amounts on or after the expiration timestamp (para [0118], [0180], [0278], [0284], [0535]-[0540], [0628]).

As to claim 21, Rosen further teaches a system where: a. the terms further comprise: i. a second principal amount; and ii. an expiration timestamp; b. the first computer processor is further configured to: i. compute one or more disbursement amounts by applying a disbursement function to: A. the value from the first data source; and at least one of: I. the first principal amount; and II. the second principal amount; ii. compute a second cryptographic signature from the first private key; iii. create an inchoate refund transaction record comprising: A. a commit input for receiving the commit amount from the commit transaction; B. a refund output comprising a refund amount; and C. the second cryptographic signature; and iv. publish the inchoate refund transaction record to at least one of the first client and the second client; and c. the inchoate disbursement transaction record further comprises one or more disbursement outputs comprising the disbursement amounts (para [0157]-[0174], [0176]-[0179], [0251], [0300], [0535], [0791]-[0802], [0806]-[0807], [0845]).

As to claim 22, Rosen further teaches a system where: a. the terms further comprise: i. a second principal amount; and ii. an expiration timestamp; b. the first key pair sector further stores a fourth asymmetric key pair, the fourth asymmetric key pair comprising a fourth private key and a fourth public key; c. the first computer processor is further configured to: i. compute one or more disbursement amounts by applying a disbursement function to: A. the value from the first data source; and at least one of: I. the first principal amount; and II. the second principal amount; ii. read the fourth private key from the first key pair sector; iii. compute a second cryptographic signature from the fourth private key; iv. create a commit transaction record comprising: A. a first principal input for receiving the first principal amount from the first principal transaction; B. a second principal input for receiving the second principal amount from the second principal transaction; C. a commit output comprising the commit amount; and D. the second cryptographic signature; and v. create the commit transaction by submitting the commit transaction record to the transfer mechanism; and d. the inchoate disbursement transaction record further comprises one or more disbursement outputs comprising the disbursement amounts (para [0157]-[0174], [0176]-[0179], [0251], [0300], [0535], [0791]-[0802], [0806]-[0807]).

As to claim 23, Rosen further teaches a system where: a. the second computer processor is further configured to: i. compute a third cryptographic signature from the second private key; ii. create a first principal transaction record comprising: A. a first principal output comprising the first principal amount; and B. the third cryptographic signature; and iii. create a first principal transaction by submitting the first principal transaction record to the transfer mechanism; and b. the third computer processor is further configured to: i. compute a fourth cryptographic signature from the third private key; ii. create a second principal transaction record comprising: A. a second principal output comprising the second principal amount; and B. the fourth cryptographic signature; and iii. create a second principal transaction by submitting the second principal transaction record to the transfer mechanism (para [0157]-[0174], [0176]-[0179], [0300], [0490], [0662], [0791]-[0802]).

(See Next Continuation Box)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No. PCT/US 15/29196

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**

Continuation of:
Box V.2. Citations and explanations:

As to claim 24, Rosen teaches a method for facilitating value transfers via a transfer mechanism (para [0149]-[0151], [0161], Fig. 56), the transfer mechanism comprising a digital currency (para [0118]), the method comprising: a. storing a first asymmetric key pair in a first key pair sector of a first memory, the first asymmetric key pair comprising a first private key and a first public key (para [0162], [0685]-[0688], claim 1, claim 2, claim 13); b. storing a second asymmetric key pair in a second key pair sector of a second memory, the second asymmetric key pair comprising a second private key and a second public key (para [0142]-[0143], [0159], [0749], claim 91); c. storing a third asymmetric key pair in the second key pair sector, the third key pair comprising a third private key and a third public key (para [1660]-[1663], Fig. 57A); d. storing a fourth asymmetric key pair in a third key pair sector of a third memory, the fourth asymmetric key pair comprising a fourth private key and a fourth public key (para [0193], [0683]-[0688], [0854], Fig. 56, claim 13 - a plurality key pairs may be generated on demand and are transmitted/stored between multiple modules/memories); e. transmitting terms from a client via a first network interface (para [0231]-[0234]), the terms comprising: i. a first principal amount (para [0165]); and ii. a reference to a first data source (para [0159], [1297]); f. receiving the terms at a facilitator via a second network interface (para [0026], [0589], [0666]); g. reading the first private key from the first key pair sector (para [0504], claim 13); h. computing a first cryptographic signature from the first private key (para [0660], [0662], [0702]); i. creating a first principal transaction record comprising: i. a first principal output comprising the first principal amount; and ii. the first cryptographic signature (para [0157]-[0174]); j. creating a first principal transaction by submitting the first principal transaction record to the transfer mechanism (para [0546], [0791]-[0802]); k. reading the second private key from the second key pair sector (para [0630], [0664], [0749], Fig. 52); l. computing a second cryptographic signature from the second private key (para [0660], [0662]); m. creating a commit transaction record comprising: i. a first principal input for receiving the first principal amount from the first principal transaction; ii. a commit output comprising a commit amount; and iii. the second cryptographic signature; n. creating the commit transaction by submitting the commit transaction record to the transfer mechanism (para [0157]-[0174], [0176]-[0179], [0300], [0535], [0791]-[0802]); o. retrieving a value from the first data source (para [0149], [0677]); p. reading the third private key from the second key pair sector (para [0664], [1660]-[1663], Fig. 56); q. computing a third cryptographic signature from the second private key; r. creating an inchoate disbursement transaction record comprising: i. a commit input for receiving a commit amount from a commit transaction; ii. the third cryptographic signature; s. publishing the inchoate disbursement transaction record (para [0157]-[0174], [0176]-[0179], [0193], [0300], [0791]-[0802]); t. reading the inchoate disbursement transaction record; u. reading the fourth private key from the third key pair sector; v. computing a fourth cryptographic signature from the fourth private key; w. creating a complete disbursement transaction record comprising: i. the commit input; ii. the third cryptographic signature; and iii. the fourth cryptographic signature; and x. creating a disbursement transaction by submitting the complete disbursement transaction record to the transfer mechanism (para [0157]-[0174], [0176]-[0179], [0193], [0300], [0660], [0662], [0791]-[0802]), but does not explicitly teach a decentralized digital currency. However, Feigelson does teach a decentralized digital currency (para [0050]-[0051] - "currency on the Bitcoin ecurrency network"). It would have been obvious to one of ordinary skill in the art to utilize a decentralized digital currency as taught by Feigelson in order to provide a monetary system using electronic media to exchange economic value securely and reliably as taught by Rosen capable of improved transaction security and less reliance on a central currency issuer.

As to claim 25, Rosen further teaches a method further comprising the steps: a. computing a disbursement amount by applying a disbursement function to: i. the first principal amount; and ii. the value from the first data source; and where: b. the inchoate disbursement transaction record further comprises a disbursement output comprising the disbursement amount; and c. the complete disbursement transaction record further comprises the disbursement output (para [0157]-[0174], [0791]-[0802]).

As to claim 26, Rosen further teaches a method further comprising the steps: a. computing a fifth cryptographic signature from the third private key; b. creating an inchoate refund transaction record comprising: i. a commit input for receiving the commit amount from the commit transaction; ii. a refund output comprising a refund amount; iii. the fifth cryptographic signature; and iv. a lock time; and c. publishing the inchoate refund transaction record (para [0157]-[0174], [0176]-[0179], [0251], [0300], [0660], [0662], [0806]-[0807], [0845]).

As to claim 27, Rosen further teaches a method where at least one of: a. the second asymmetric key pair consists of the third asymmetric key pair, the second private key consists of the third private key, and the second public key consists of the third public key; b. the first asymmetric key pair consists of the fourth asymmetric key pair, the first private key consists of the fourth private key, and the first public key consists of the fourth public key; and c. the first memory consists of the third memory and the first key pair sector consists of the third key pair sector (claim1, claim 2, claim 13 - "generating a device key pair for said device, said device key pair including a device private key and a device public key which are stored in a memory"; "a key pair regenerator for forming a new key pair, upon an occurrence of a predetermined event, where said key pair includes a new public key and a new private key" - memory, which may be divided into addressable sectors/blocks, could include the various generated key pairs; the overarching memory architecture itself containing all individual sectors/blocks (e.g. memory 1 could consist of several subunits of memory, such as memory 2, memory 3, etc., each subunit representing a sector containing a key pair value)).

As to claim 28, Rosen further teaches a method further comprising the steps: a. storing a fifth asymmetric key pair in a fourth key pair sector of a fourth memory, the fifth asymmetric key pair comprising a fifth private key and a fifth public key; b. reading the fifth private key from the fourth key pair sector; c. computing a fifth cryptographic signature from the fifth private key; d. creating a second principal transaction record comprising: i. a second principal output comprising the second principal amount; and ii. the fifth cryptographic signature; e. creating a second principal transaction by submitting the second principal transaction record to the transfer mechanism; f. computing one or more disbursement amounts by applying a disbursement function to: i. the value from the first data source; and at least one of: A. the first principal amount; and B. the second principal amount; and where: g. the inchoate disbursement transaction record further comprises one or more disbursement outputs comprising the disbursement amounts; and h. the complete disbursement transaction record further comprises the disbursement outputs (para [0157]-[0174], [0176]-[0179], [0288], [0504], [0535], [0546], [0791]-[0802]).

(See Next Continuation Box)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 15/29196

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:
Box V.2. Citations and explanations:

As to claim 29, Rosen further teaches a method further comprising the steps: a. computing a sixth cryptographic signature from the third private key; b. creating an inchoate refund transaction record comprising: i. a commit input for receiving the commit amount from the commit transaction; ii. one or more refund outputs comprising one or more refund amounts; iii. the sixth cryptographic signature; and iv. a lock time; and c. publishing the inchoate refund transaction record (para [0157]-[0174], [0176]-[0179], [0251], [0300], [0660], [0662], [0806]-[0807], [0845] - computing of cryptographic signatures can be accomplished for any of a plurality of trusted agents' private keys, which can then be included in subsequent transaction logs/records).

As to claim 30, Rosen further teaches a method where at least one of: a. the second asymmetric key pair consists of the third asymmetric key pair, the second private key consists of the third private key, and the second public key consists of the third public key; b. the first asymmetric key pair consists of the fourth asymmetric key pair, the first private key consists of the fourth private key, and the first public key consists of the fourth public key; c. the fifth asymmetric key pair consists of the fourth asymmetric key pair, the fifth private key consists of the fourth private key, and the fifth public key consists of the fourth public key; d. the first memory consists of the third memory and the first key pair sector consists of the third key pair sector; and e. the fifth memory consists of the third memory and the fifth key pair sector consists of the third key pair sector (claim1, claim 2, claim 13 - "generating a device key pair for said device, said device key pair including a device private key and a device public key which are stored in a memory"; "a key pair regenerator for forming a new key pair, upon an occurrence of a predetermined event, where said key pair includes a new public key and a new private key" - memory, which may be divided into addressable sectors/blocks, could include the various generated key pairs; the overarching memory architecture itself containing all individual sectors/blocks (e.g. memory 1 could consist of several subunits of memory, such as memory 2, memory 3, etc., each subunit representing a sector containing a key pair value)).

Claims 1-30 have industrial applicability as defined by PCT Article 33(4) because the subject matter can be made or used in industry.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 November 2015 (12.11.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/171580 A1

(51) International Patent Classification:
H04L 29/06 (2006.01)

(21) International Application Number:
PCT/US2015/029196

(22) International Filing Date:
5 May 2015 (05.05.2015)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/990,795 9 May 2014 (09.05.2014) US

(71) Applicant: **VERITASEUM, INC.** [US/US]; 195 Argyle Rd, Brooklyn, NY 11218 (US).

(72) Inventors; and
(71) Applicants : **MIDDLETON, Regginald** [US/US]; 195 Argyle Rd, Brooklyn, NY 11218 (US). **BOGOSIAN, Matthew** [US/US]; 5007 Totem Trl, Anacortes, WA 98221 (US).

(74) Agent: **NIELSEN, John, E.**; Sentinel IP, PC, 484 Washington St, Suite B-345, Monterey, CA 93940 (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:
— *with international search report (Art. 21(3))*

(54) **Title**: DEVICES, SYSTEMS, AND METHODS FOR FACILITATING LOW TRUST AND ZERO TRUST VALUE TRANSFERS

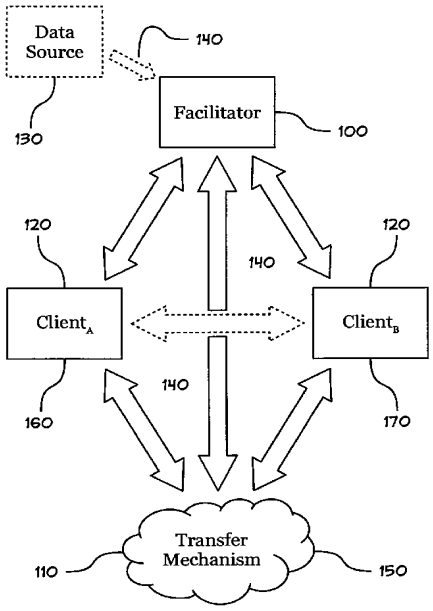


FIG. 1

(57) **Abstract**: Devices, systems, and methods enabling parties with little trust or no trust in each other to enter into and enforce value transfer agreements conditioned on input from or participation of a third party, over arbitrary distances, without special technical knowledge of the underlying transfer mechanism(s), optionally affording participation of third-party mediators, substitution of transferors and transferees, term substitution, revision, or reformation, etc. Such value transfers can occur reliably without involving costly third-party intermediaries who traditionally may otherwise be required, and without traditional exposure to counterparty risk.

WO 2015/171580 A1

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. 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	2626.P100.US
	Application Number	
Title of Invention	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers	

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
	Reginald		Middleton	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Brooklyn	State/Province	NY	Country of Residence	US

Mailing Address of Inventor:

Address 1	195 Argyle Road		
Address 2			
City	Brooklyn	State/Province	NY
Postal Code	11218	Country	US

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Matthew		Bogosian	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Anacortes	State/Province	WA	Country of Residence	US

Mailing Address of Inventor:

Address 1	5007 Totem Trl		
Address 2			
City	Anacortes	State/Province	WA
Postal Code	98221	Country	US

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).

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. 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	2626.P100.US
	Application Number	
Title of Invention	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers	

☐ An Address is being provided for the correspondence Information of this application.			
Customer Number	115238		
Email Address		Add Email	Remove Email

Application Information:

Title of the Invention	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers		
Attorney Docket Number	2626.P100.US	**Small Entity Status Claimed** ☒	
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	16	**Suggested Figure for Publication (if any)**	1

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.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	115238		

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	2626.P100.US
	Application Number	
Title of Invention	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers	

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)
PCT/US15/29196	a 371 of international		2015-05-05
Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
61/990795	Claims benefit of provisional		2014-05-09

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.

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)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button.

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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	2626.P100.US
	Application Number	
Title of Invention	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers	

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 (11-15)
Approved for use through 04/30/2017. 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	2626.P100.US
	Application Number	
Title of Invention	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers	

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

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	Veritaseum, Inc.		
Mailing Address Information For Applicant:			
Address 1	195 Argyle Road		
Address 2			
City	Brooklyn	**State/Province**	NY
Country	US	Postal Code	11218
Phone Number	718-407-4756	Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button.

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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	2626.P100.US
	Application Number	
Title of Invention	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers	

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.

If the Assignee or Non-Applicant Assignee is an Organization check here. ☒

Organization Name	

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.

Signature:

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	/JohnNielsen53392/			Date (YYYY-MM-DD)	2016-11-04
First Name	John	Last Name	Nielsen	Registration Number	53,392

Additional Signature may be generated within this form by selecting the Add button.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. 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	2626.P100.US
	Application Number	
Title of Invention	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers	

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.**

CLAIMS

What is claimed is:

1. A device for facilitating a value transfer between a first party utilizing a first client and a second party utilizing a second client via a transfer mechanism, the device comprising:

a. a first memory comprising a transaction record sector and a first key pair sector for storing a first asymmetric key pair, the first asymmetric key pair comprising a first private key and a first public key;

b. a first network interface for receiving terms, the terms comprising:

i. a first principal amount; and

ii. a reference to a first data source; and

c. a first computer processor coupled to the first memory and the first network interface, the first computer processor configured to:

i. retrieve a value from the first data source;

ii. read the first private key from the first key pair sector;

iii. compute a first cryptographic signature from the first private key;

iv. create an inchoate disbursement transaction record comprising:

A. a commit input for receiving a commit amount from a commit transaction; and

B. the first cryptographic signature; and

v. publish the inchoate disbursement transaction record to at least one of the first client and the second client;

where the first client comprises:

a. a second memory comprising a second key pair sector for storing a second asymmetric key pair, the second asymmetric key pair comprising a second private key and a second public key;

b. a second network interface; and

c. a second computer processor coupled to the second memory and the second network interface, the second computer processor configured to read the second private key from the second key pair sector; and

where the second client comprises;

a. a third memory comprising a third key pair sector for storing a third asymmetric key pair, the third asymmetric key pair comprising a third private key and a third public key;

b. a third network interface; and

c. a third computer processor coupled to the third memory and the third network interface, the third computer processor configured to read the third private key from the third key pair sector.

2. The device of claim 1, where the transfer mechanism comprises a decentralized digital currency.

3. The device of claim 1, where:

a. the first computer processor is further configured to compute a disbursement amount by applying a disbursement function to:

i. the first principal amount; and

ii. the value from the first data source; and

b. the inchoate disbursement transaction record further comprises a disbursement output comprising the disbursement amount.

4. The device of claim 3, where the first computer processor is further configured to:

a. compute a second cryptographic signature from the first private key;

b. create an inchoate refund transaction record comprising:

i. a commit input for receiving the commit amount from the commit transaction;

ii. a refund output comprising a refund amount;

iii. the second cryptographic signature; and

iv. a lock time; and

c. publish the inchoate refund transaction record to at least one of the first client or the second client.

5. The device of claim 3, where:

a. the first key pair sector further stores a fourth asymmetric key pair, the fourth asymmetric key pair comprising a fourth private key and a fourth public key; and

b. the first computer processor is further configured to:

i. read the fourth private key from the first key pair sector;

ii. compute a second cryptographic signature from the fourth private key;

iii. create a commit transaction record, the commit transaction record comprising:

A. a first principal input for receiving the first principal amount from a first principal transaction;

B. a commit output comprising the commit amount;

C. the second cryptographic signature; and

iv. create the commit transaction by submitting the commit transaction record to the transfer mechanism.

6. The device of claim 5, where the first asymmetric key pair consists of the fourth asymmetric key pair, the first private key consists of the fourth private key, and the first public key consists of the fourth public key.

7. The device of claim 1, where:

a. the terms further comprise:

i. a second principal amount; and

ii. an expiration timestamp;

b. the first computer processor is further configured to compute the one or more disbursement amounts by applying a disbursement function to:

i. the value from the first data source; and at least one of:

A. the first principal amount; and

B. the second principal amount; and

c. the inchoate disbursement transaction record further comprises one or more disbursement outputs comprising the disbursement amounts.

8. The device of claim 7, where:

a. the terms further comprise:

i. a reference to a second data source;

b. the first computer processor is further configured to compute the one or more disbursement amounts by applying the disbursement function to:

i. the value from the first data source;

ii. the value from the second data source;

iii. the first principal amount; and

iv. the second principal amount.

9. The device of claim 7, where:

a. the reference to the first data source comprises at least one of a reference to a base instrument and a reference to a quote instrument; and

b. the first computer processor is further configured to compute the disbursement amounts on or after the expiration timestamp.

10. The device of claim 7, where the first computer processor is further configured to:

a. compute a second cryptographic signature from the first private key;

b. create an inchoate refund transaction record comprising:

i. a commit input for receiving the commit amount from the commit transaction;

ii. one or more refund outputs comprising one or more refund amounts;

iii. the second cryptographic signature; and

iv. a lock time; and

c. publish the inchoate refund transaction record to at least one of the first client and the second client.

11. The device of claim 7, where:

a. the first key pair sector further stores a fourth asymmetric key pair, the fourth asymmetric key pair comprising a fourth private key and a fourth public key; and

b. the first computer processor is further configured to:

i. read the fourth private key from the first key pair sector;

ii. compute a second cryptographic signature from the fourth private key;

iii. create a commit transaction record comprising:

A. a first principal input for receiving the first principal amount from a first principal transaction;

B. a second principal input for receiving the second principal amount from a second principal transaction;

C. a commit output comprising a commit amount; and

D. the second cryptographic signature; and

iv. create the commit transaction by submitting the commit transaction record to the transfer mechanism.

12. A system for facilitating a value transfer between a first party utilizing a first client and a second party utilizing a second client via a transfer mechanism, the transfer mechanism comprising a decentralized digital currency, the system comprising a facilitator, the first client, and the second client;

a. the facilitator comprising:

i. a first memory comprising a transaction record sector and a first key pair sector for storing a first asymmetric key pair, the first asymmetric key pair comprising a first private key and a first public key;

ii. a first network interface for receiving terms, the terms comprising:

A. a first principal amount; and

B. a reference to a first data source; and

iii. a first computer processor coupled to the first memory and the first network interface, the first computer processor configured to:

A. retrieve a value from the first data source;

B. read the first private key from the first key pair sector;

C. compute a first cryptographic signature from the first private key;

D. create an inchoate disbursement transaction record comprising:

I. a commit input for receiving a commit amount from a commit transaction; and

II. the first cryptographic signature; and

E. publish the inchoate disbursement transaction record to at least one of the first client and the second client;

b. the first client comprising:

i. a second memory comprising a second key pair sector for storing a second asymmetric key pair, the second asymmetric key pair comprising a second private key and a second public key;

ii. a second network interface; and

iii. a second computer processor coupled to the second memory and the second network interface, the second computer processor configured to read the second private key from the second key pair sector; and

c. the second client comprising:

i. a third memory comprising a third key pair sector for storing a third asymmetric key pair, the third asymmetric key pair comprising a third private key and a third public key;

ii. a third network interface; and

iii. a third computer processor coupled to the third memory and the third network interface, the third computer processor configured to read the third private key from the third key pair sector.

13. The system of claim 12, where:

a. the first computer processor consists of the second computer processor;

b. the first memory consists of the second memory; and

c. the first network interface consists of the second network interface.

14. The system of claim 12, where:

a. the first computer processor is further configured compute a disbursement amount by applying a disbursement function to:

i. the first principal amount; and

ii. the value from the first data source;

b. the inchoate disbursement transaction record further comprises a disbursement output comprising the disbursement amount; and

c. the second computer processor is further configured to:

i. read the inchoate disbursement transaction;

ii. compute a second cryptographic signature from the second private key;

iii. create a complete disbursement transaction record comprising:

A. the commit input;

B. the disbursement output;

C. the first cryptographic signature; and

D. the second cryptographic signature; and

iv. create a disbursement transaction by submitting the complete disbursement transaction record to the transfer mechanism.

15. The system of claim 12, where the first computer processor is further configured to:

a. compute a second cryptographic signature from the first private key;

b. create an inchoate refund transaction record comprising:

i. a commit input for receiving the commit amount from the commit transaction;

ii. a refund output comprising a refund amount; and

iii. the second cryptographic signature; and

c. publish the inchoate refund transaction record to at least one of the first client and the second client.

16. The system of claim 12, where:

a. the first key pair sector further stores a fourth asymmetric key pair, the fourth asymmetric key pair comprising a fourth private key and a fourth public key;

b. the first computer processor is further configured to:

i. compute a disbursement amount by applying a disbursement function to:

A. the first principal amount; and

B. the value from the first data source;

ii. read the fourth private key from the first key pair sector;

iii. compute a second cryptographic signature from the fourth private key;

iv. create a commit transaction record comprising:

A. a first principal input for receiving the first principal amount from a first principal transaction;

B. a commit output comprising the commit amount; and

C. the second cryptographic signature; and

v. create the commit transaction by submitting the commit transaction record to the transfer mechanism; and

c. the inchoate disbursement transaction record further comprises a disbursement output comprising the disbursement amount.

17. The system of claim 16, where the second computer processor is configured to:

a. compute a third cryptographic signature from the second private key;

b. create a first principal transaction record comprising:

i. a first principal output comprising the first principal amount; and

ii. the third cryptographic signature; and

c. create the first principal transaction by submitting the first principal transaction record to the transfer mechanism.

18. The system of claim 12, where:

a. the terms further comprise:

i. a second principal amount; and

ii. an expiration timestamp;

b. the first computer processor is further configured compute one or more disbursement amounts by applying a disbursement function to:

i. the value from the first data source; and at least one of:

A. the first principal amount; and

B. the second principal amount;

c. the inchoate disbursement transaction record further comprises one or more disbursement outputs comprising the disbursement amounts; and

d. the second computer processor is further configured to:

i. read the inchoate disbursement transaction;

ii. compute a second cryptographic signature from the second private key;

iii. create a complete disbursement transaction record comprising:

A. the commit input;

B. the disbursement outputs;

C. the first cryptographic signature; and

D. the second cryptographic signature; and

iv. create a disbursement transaction by submitting the complete disbursement transaction record to the transfer mechanism.

19. The system of claim 18, where:

a. the terms further comprise:

i. a reference to a second data source;

b. the first computer processor is further configured to compute the one or more disbursement amounts by applying the disbursement function to:

i. the value from the first data source;

ii. the value from the second data source;

iii. the first principal amount; and

iv. the second principal amount.

20. The system of claim 18, where:

a. the reference to the first data source comprises at least one of a reference to a base instrument and a reference to a quote instrument; and

b. the first computer processor is further configured to compute the disbursement amounts on or after the expiration timestamp.

21. The system of claim 12, where:

a. the terms further comprise:

i. a second principal amount; and

ii. an expiration timestamp;

b. the first computer processor is further configured to:

i. compute one or more disbursement amounts by applying a disbursement function to:

A. the value from the first data source; and at least one of:

I. the first principal amount; and

II. the second principal amount;

ii. compute a second cryptographic signature from the first private key;

iii. create an inchoate refund transaction record comprising:

A. a commit input for receiving the commit amount from the commit transaction;

B. a refund output comprising a refund amount; and

C. the second cryptographic signature; and

iv. publish the inchoate refund transaction record to at least one of the first client and the second client; and

c. the inchoate disbursement transaction record further comprises one or more disbursement outputs comprising the disbursement amounts.

22. The system of claim 12, where:

a. the terms further comprise:

i. a second principal amount; and

ii. an expiration timestamp;

b. the first key pair sector further stores a fourth asymmetric key pair, the fourth asymmetric key pair comprising a fourth private key and a fourth public key;

c. the first computer processor is further configured to:

i. compute one or more disbursement amounts by applying a disbursement function to:

A. the value from the first data source; and at least one of:

I. the first principal amount; and

II. the second principal amount;

ii. read the fourth private key from the first key pair sector;

iii. compute a second cryptographic signature from the fourth private key;

iv. create a commit transaction record comprising:

A. a first principal input for receiving the first principal amount from the first principal transaction;

B. a second principal input for receiving the second principal amount from the second principal transaction;

C. a commit output comprising the commit amount; and

D. the second cryptographic signature; and

v. create the commit transaction by submitting the commit transaction record to the transfer mechanism; and

d. the inchoate disbursement transaction record further comprises one or more disbursement outputs comprising the disbursement amounts.

23. The system of claim 22, where:

a. the second computer processor is further configured to:

i. compute a third cryptographic signature from the second private key;

ii. create a first principal transaction record comprising:

A. a first principal output comprising the first principal amount; and

B. the third cryptographic signature; and

iii. create a first principal transaction by submitting the first principal transaction record to the transfer mechanism; and

b. the third computer processor is further configured to:

i. compute a fourth cryptographic signature from the third private key;

ii. create a second principal transaction record comprising:

A. a second principal output comprising the second principal amount; and

B. the fourth cryptographic signature; and

iii. create a second principal transaction by submitting the second principal transaction record to the transfer mechanism.

24. A method for facilitating value transfers via a transfer mechanism, the transfer mechanism comprising a decentralized digital currency, the method comprising:

a. storing a first asymmetric key pair in a first key pair sector of a first memory, the first asymmetric key pair comprising a first private key and a first public key;

b. storing a second asymmetric key pair in a second key pair sector of a second memory, the second asymmetric key pair comprising a second private key and a second public key;

c. storing a third asymmetric key pair in the second key pair sector, the third key pair comprising a third private key and a third public key;

d. storing a fourth asymmetric key pair in a third key pair sector of a third memory, the fourth asymmetric key pair comprising a fourth private key and a fourth public key;

e. transmitting terms from a client via a first network interface, the terms comprising:

i. a first principal amount; and

ii. a reference to a first data source;

f. receiving the terms at a facilitator via a second network interface;

g. reading the first private key from the first key pair sector;

h. computing a first cryptographic signature from the first private key;

i. creating a first principal transaction record comprising:

i. a first principal output comprising the first principal amount; and

ii. the first cryptographic signature;

j. creating a first principal transaction by submitting the first principal transaction record to the transfer mechanism;

k. reading the second private key from the second key pair sector;

l. computing a second cryptographic signature from the second private key;

m. creating a commit transaction record comprising:

i. a first principal input for receiving the first principal amount from the first principal transaction;

ii. a commit output comprising a commit amount; and

iii. the second cryptographic signature;

n. creating the commit transaction by submitting the commit transaction record to the transfer mechanism;

o. retrieving a value from the first data source;

p. reading the third private key from the second key pair sector;

q. computing a third cryptographic signature from the second private key;

r. creating an inchoate disbursement transaction record comprising:

i. a commit input for receiving a commit amount from a commit transaction;

ii. the third cryptographic signature;

s. publishing the inchoate disbursement transaction record;

t. reading the inchoate disbursement transaction record;

u. reading the fourth private key from the third key pair sector;

v. computing a fourth cryptographic signature from the fourth private key;

w. creating a complete disbursement transaction record comprising:

i. the commit input;

ii. the third cryptographic signature; and

iii. the fourth cryptographic signature; and

x. creating a disbursement transaction by submitting the complete disbursement transaction record to the transfer mechanism.

25. The method of claim 24, further comprising the steps:

a. computing a disbursement amount by applying a disbursement function to:

i. the first principal amount; and

ii. the value from the first data source; and

where:

b. the inchoate disbursement transaction record further comprises a disbursement output comprising the disbursement amount; and

c. the complete disbursement transaction record further comprises the disbursement output.

26. The method of claim 25, further comprising the steps:

a. computing a fifth cryptographic signature from the third private key;

b. creating an inchoate refund transaction record comprising:

i. a commit input for receiving the commit amount from the commit transaction;

ii. a refund output comprising a refund amount;

iii. the fifth cryptographic signature; and

iv. a lock time; and

c. publishing the inchoate refund transaction record.

27. The method of claim 25, where at least one of:

a. the second asymmetric key pair consists of the third asymmetric key pair, the second private key consists of the third private key, and the second public key consists of the third public key;

b. the first asymmetric key pair consists of the fourth asymmetric key pair, the first private key consists of the fourth private key, and the first public key consists of

the fourth public key; and

c. the first memory consists of the third memory and the first key pair sector consists of the third key pair sector.

28. The method of claim 24, further comprising the steps:

a. storing a fifth asymmetric key pair in a fourth key pair sector of a fourth memory, the fifth asymmetric key pair comprising a fifth private key and a fifth public key;

b. reading the fifth private key from the fourth key pair sector;

c. computing a fifth cryptographic signature from the fifth private key;

d. creating a second principal transaction record comprising:

i. a second principal output comprising the second principal amount; and

ii. the fifth cryptographic signature;

e. creating a second principal transaction by submitting the second principal transaction record to the transfer mechanism;

f. computing one or more disbursement amounts by applying a disbursement function to:

i. the value from the first data source; and at least one of:

A. the first principal amount; and

B. the second principal amount; and

where:

g. the inchoate disbursement transaction record further comprises one or more disbursement outputs comprising the disbursement amounts; and

h. the complete disbursement transaction record further comprises the disbursement outputs.

29. The method of claim 28, further comprising the steps:

a. computing a sixth cryptographic signature from the third private key;

b. creating an inchoate refund transaction record comprising:

i. a commit input for receiving the commit amount from the commit transaction;

ii. one or more refund outputs comprising one or more refund amounts;

iii. the sixth cryptographic signature; and

iv. a lock time; and

c. publishing the inchoate refund transaction record.

30. The method of claim 28, where at least one of:

a. the second asymmetric key pair consists of the third asymmetric key pair, the second private key consists of the third private key, and the second public key consists of the third public key;

b. the first asymmetric key pair consists of the fourth asymmetric key pair, the first private key consists of the fourth private key, and the first public key consists of the fourth public key;

c. the fifth asymmetric key pair consists of the fourth asymmetric key pair, the fifth private key consists of the fourth private key, and the fifth public key consists of the fourth public key;

d. the first memory consists of the third memory and the first key pair sector consists of the third key pair sector; and

e. the fifth memory consists of the third memory and the fifth key pair sector consists of the third key pair sector.

Drawing Sheet 1 of 16

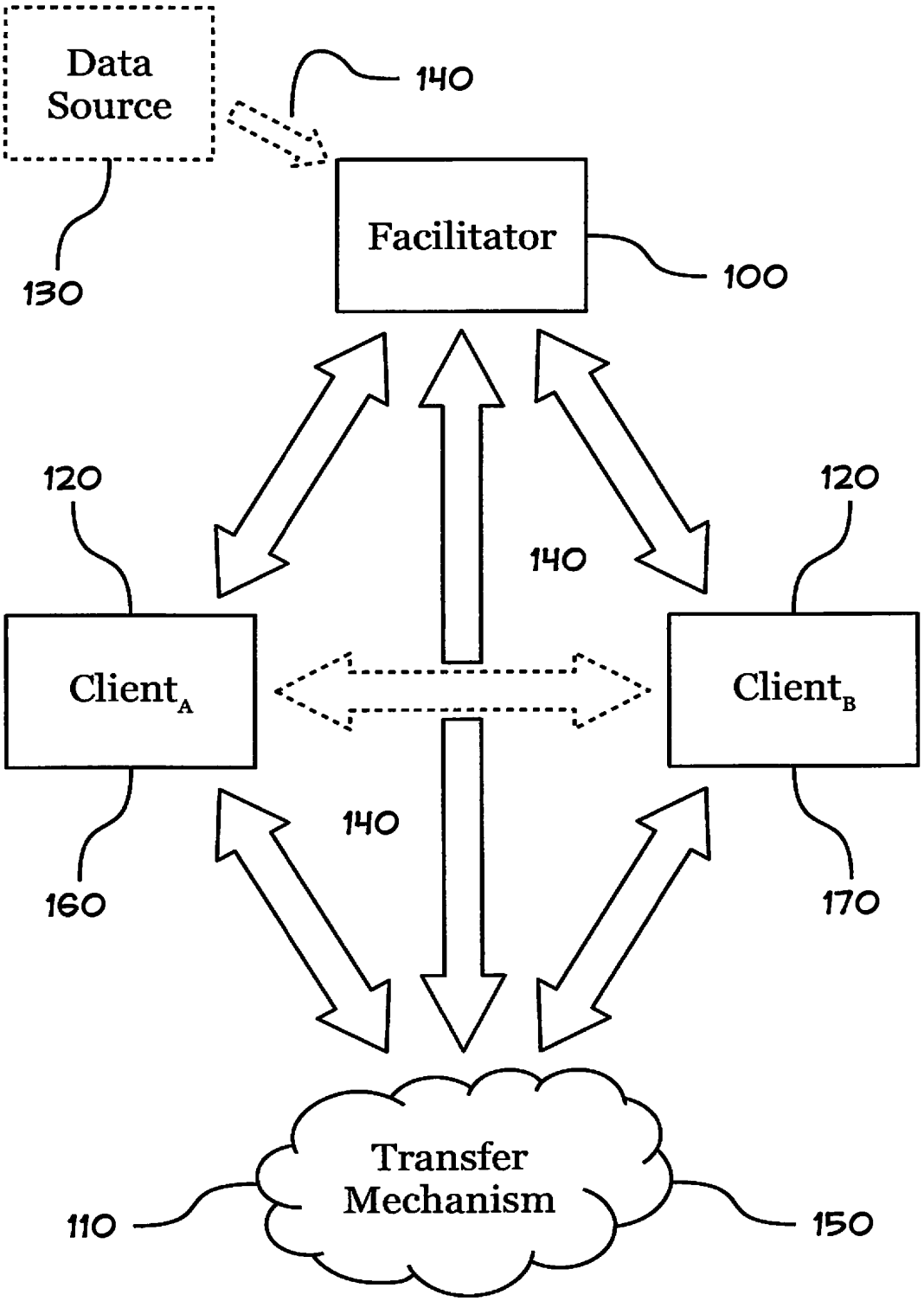


FIG. 1

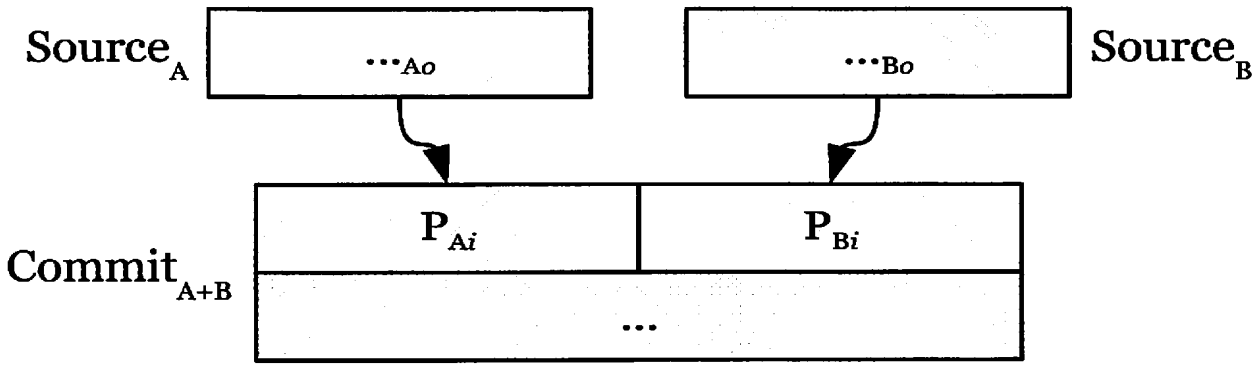

Source A
...Ao
...Bo
Source B
Commit A+B
P Ai
P Bi
...

FIG. 2

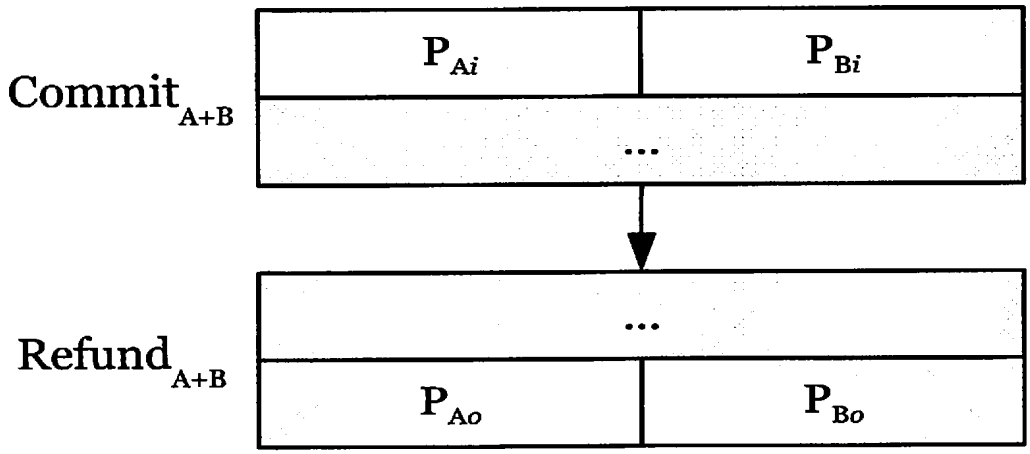

Commit A+B
P Ai
P Bi
...
Refund A+B
...
P Ao
P Bo

FIG. 3

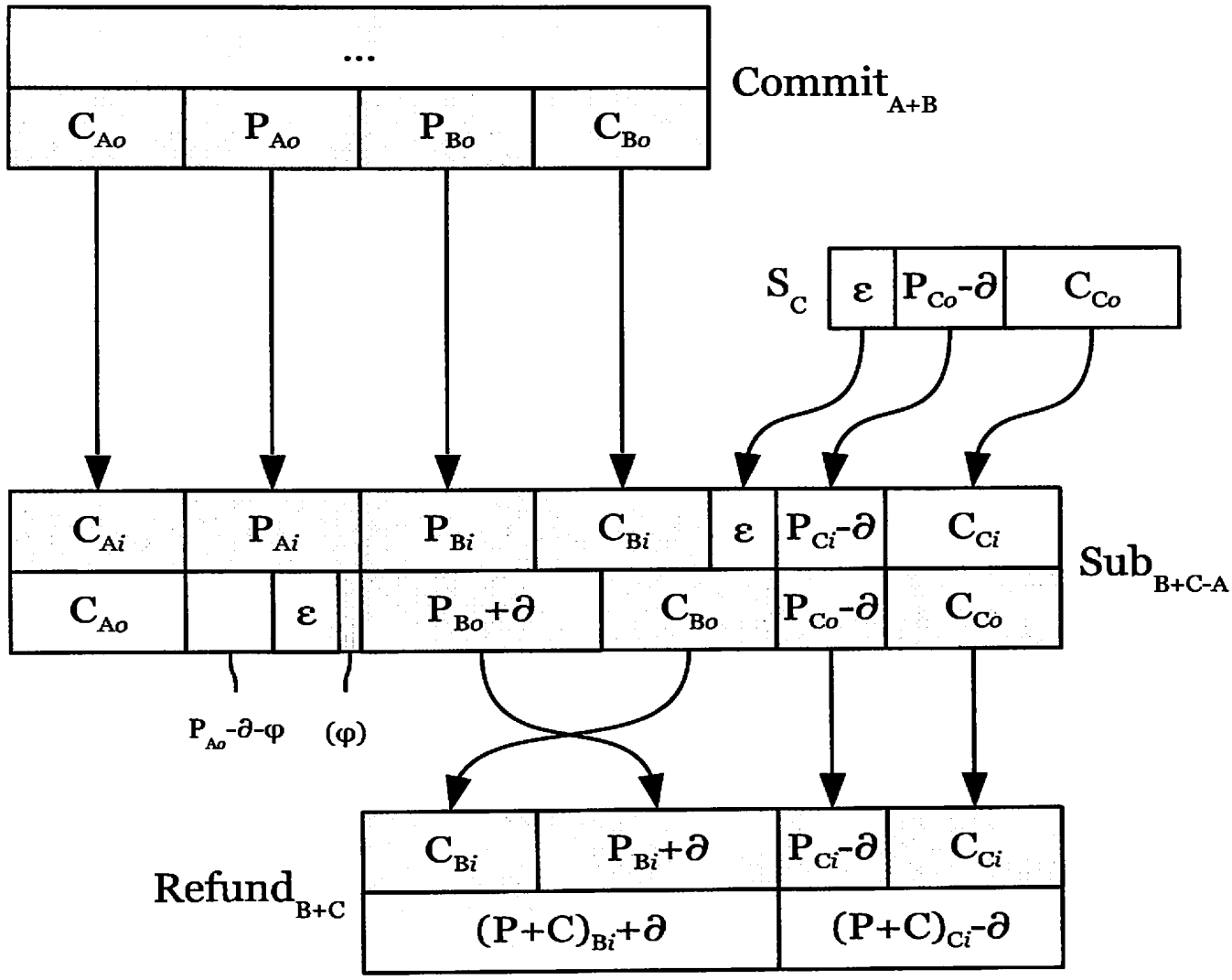

...
C_{Ao} P_{Ao} P_{Bo} C_{Bo}
$Commit_{A+B}$
S_C ε P_{Co}-∂ C_{Co}
C_{Ai} P_{Ai} P_{Bi} C_{Bi} ε P_{Ci}-∂ C_{Ci}
C_{Ao} ε P_{Bo}+∂ C_{Bo} P_{Co}-∂ C_{Co}
Sub_{B+C-A}
P_{Ao}-∂-φ (φ)
C_{Bi} P_{Bi}+∂ P_{Ci}-∂ C_{Ci}
$(P+C)_{Bi}$+∂ $(P+C)_{Ci}$-∂
$Refund_{B+C}$

FIG. 6

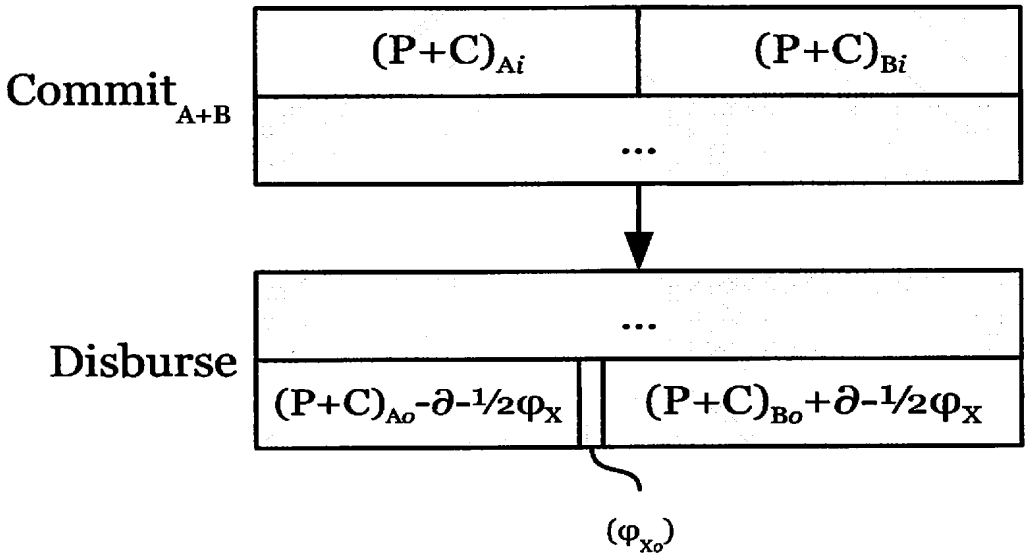

Commit A+B
(P+C)Ai
(P+C)Bi
...
Disburse
...
(P+C)Ao-∂-½φX
(P+C)Bo+∂-½φX
(φXo)

FIG. 4

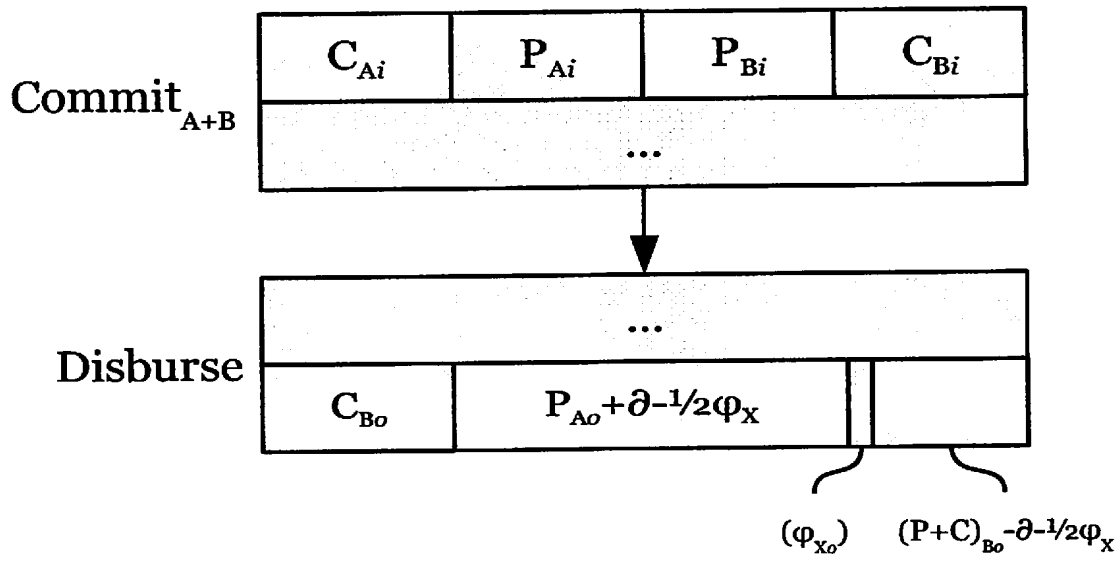

Commit A+B
CAi
PAi
PBi
CBi
...
Disburse
...
CBo
PAo+∂-½φX
(φXo)
(P+C)Bo-∂-½φX

FIG. 5

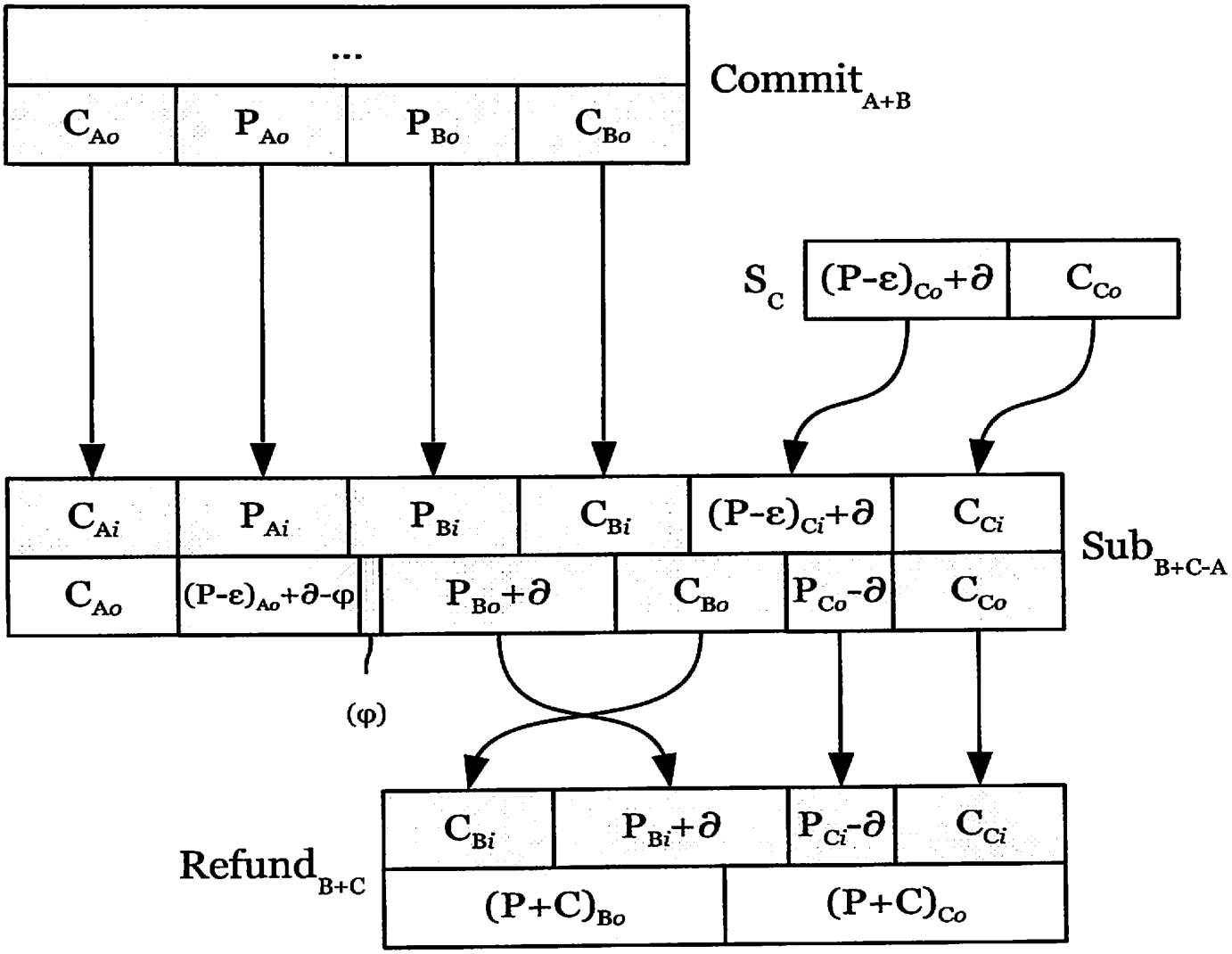

...
C_{Ao}
P_{Ao}
P_{Bo}
C_{Bo}
$Commit_{A+B}$
S_C
$(P-\varepsilon)_{Co}+\partial$
C_{Co}
C_{Ai}
P_{Ai}
P_{Bi}
C_{Bi}
$(P-\varepsilon)_{Ci}+\partial$
C_{Ci}
Sub_{B+C-A}
C_{Ao}
$(P-\varepsilon)_{Ao}+\partial-\varphi$
$P_{Bo}+\partial$
C_{Bo}
$P_{Co}-\partial$
C_{Co}
(φ)
C_{Bi}
$P_{Bi}+\partial$
$P_{Ci}-\partial$
C_{Ci}
$Refund_{B+C}$
$(P+C)_{Bo}$
$(P+C)_{Co}$

FIG. 7

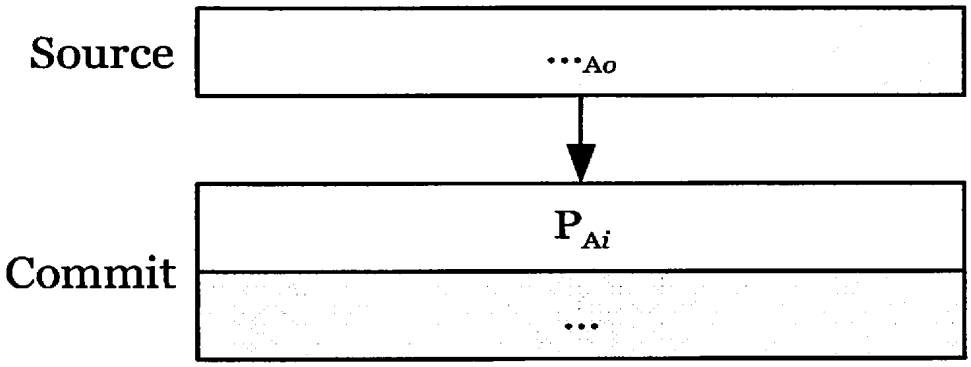


FIG. 8

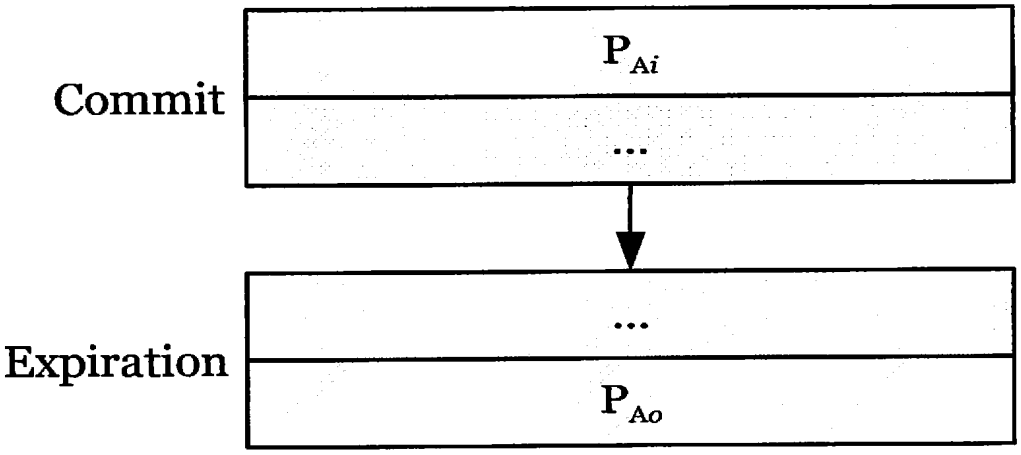


FIG. 9

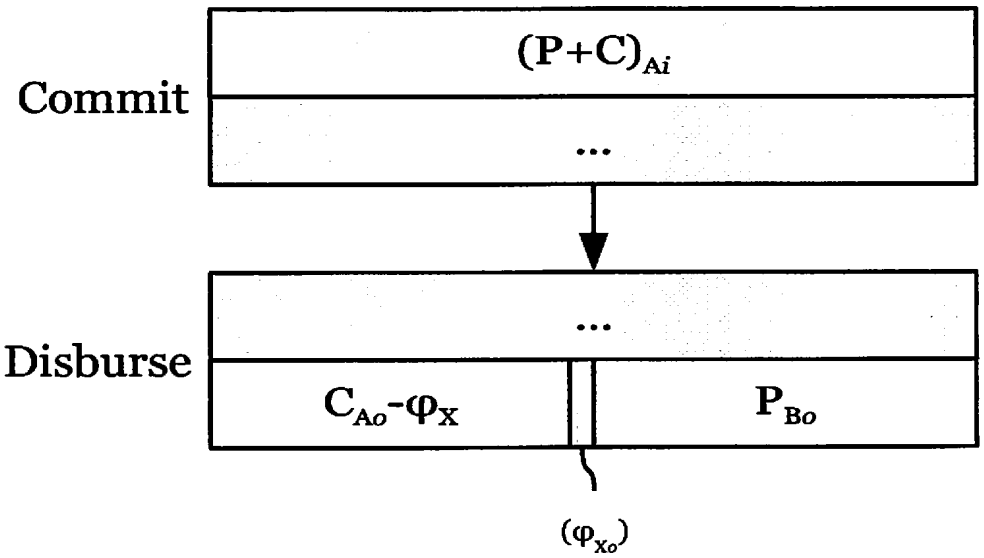

Commit
$(P+C)_{Ai}$
...
Disburse
...
$C_{Ao}-\varphi_X$
P_{Bo}
(φ_{Xo})

FIG. 10

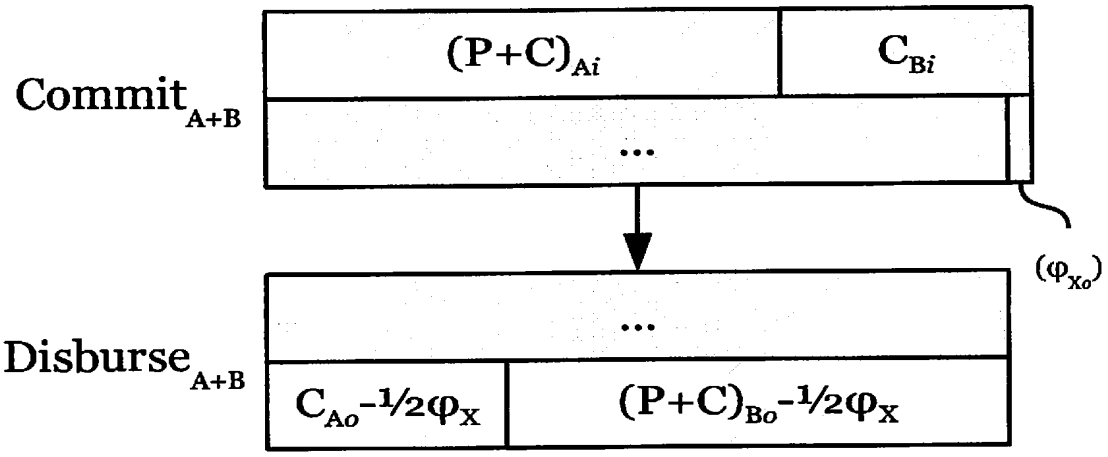

$Commit_{A+B}$
$(P+C)_{Ai}$
C_{Bi}
...
(φ_{Xo})
$Disburse_{A+B}$
...
$C_{Ao}-1/2\varphi_X$
$(P+C)_{Bo}-1/2\varphi_X$

FIG. 11

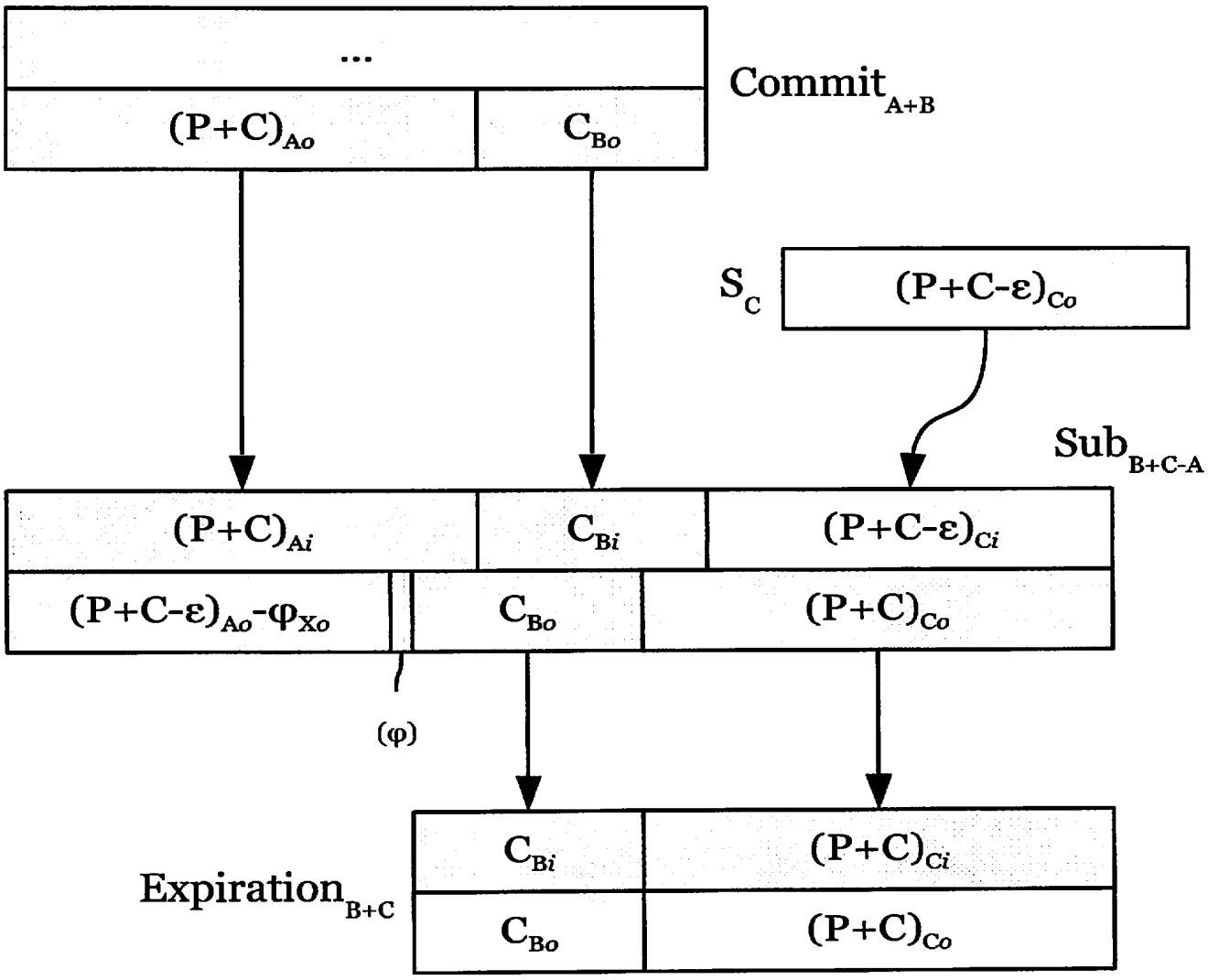

...
$(P+C)_{Ao}$
C_{Bo}
$Commit_{A+B}$
S_C
$(P+C-\varepsilon)_{Co}$
Sub_{B+C-A}
$(P+C)_{Ai}$
C_{Bi}
$(P+C-\varepsilon)_{Ci}$
$(P+C-\varepsilon)_{Ao}-\varphi_{Xo}$
C_{Bo}
$(P+C)_{Co}$
(φ)
$Expiration_{B+C}$
C_{Bi}
$(P+C)_{Ci}$
C_{Bo}
$(P+C)_{Co}$

FIG. 12

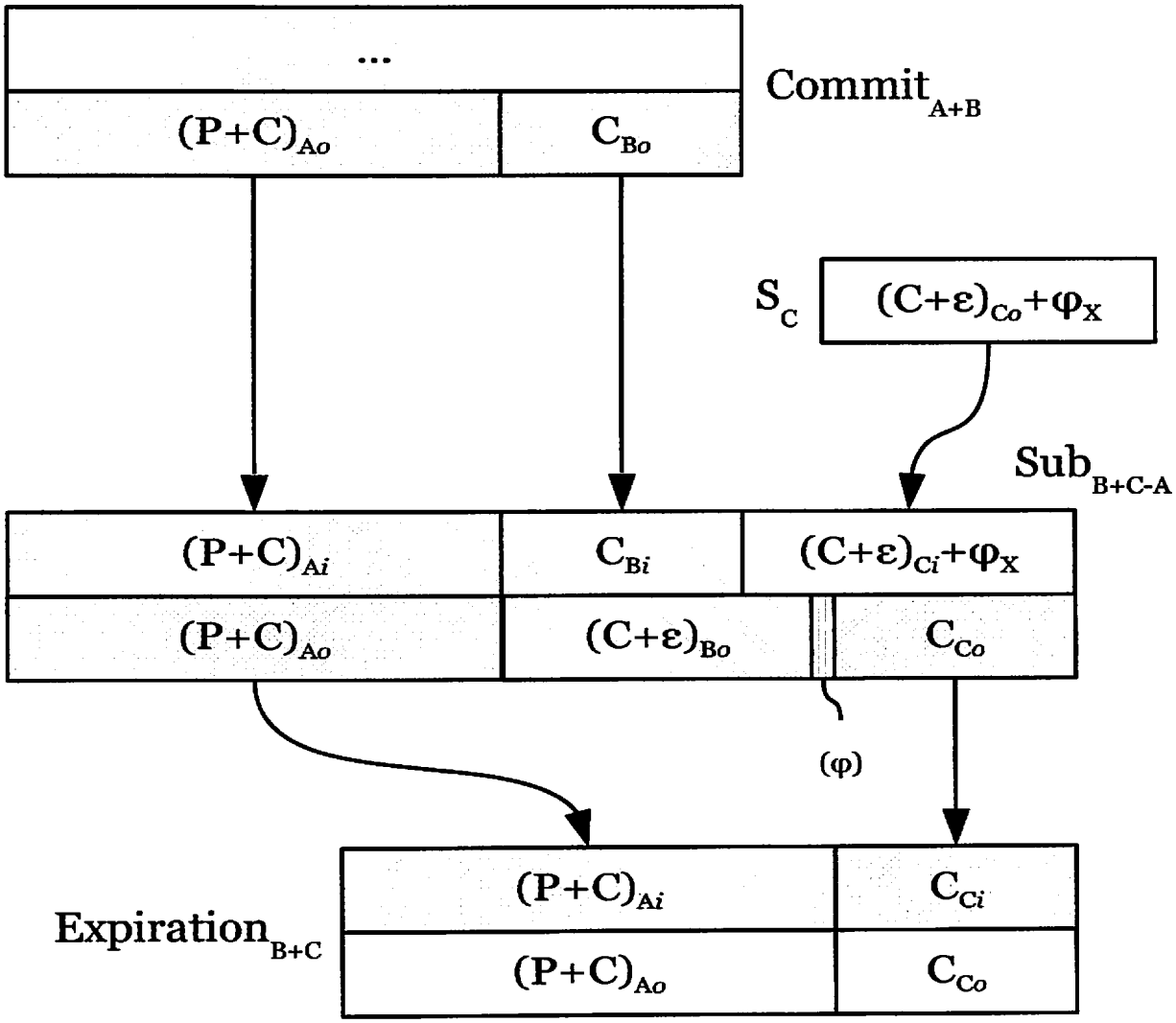

...
$(P+C)_{Ao}$
C_{Bo}
$Commit_{A+B}$
S_C
$(C+\varepsilon)_{Co}+\varphi_X$
Sub_{B+C-A}
$(P+C)_{Ai}$
C_{Bi}
$(C+\varepsilon)_{Ci}+\varphi_X$
$(P+C)_{Ao}$
$(C+\varepsilon)_{Bo}$
C_{Co}
(φ)
$Expiration_{B+C}$
$(P+C)_{Ai}$
C_{Ci}
$(P+C)_{Ao}$
C_{Co}

FIG. 13

Drawing Sheet 10 of 16

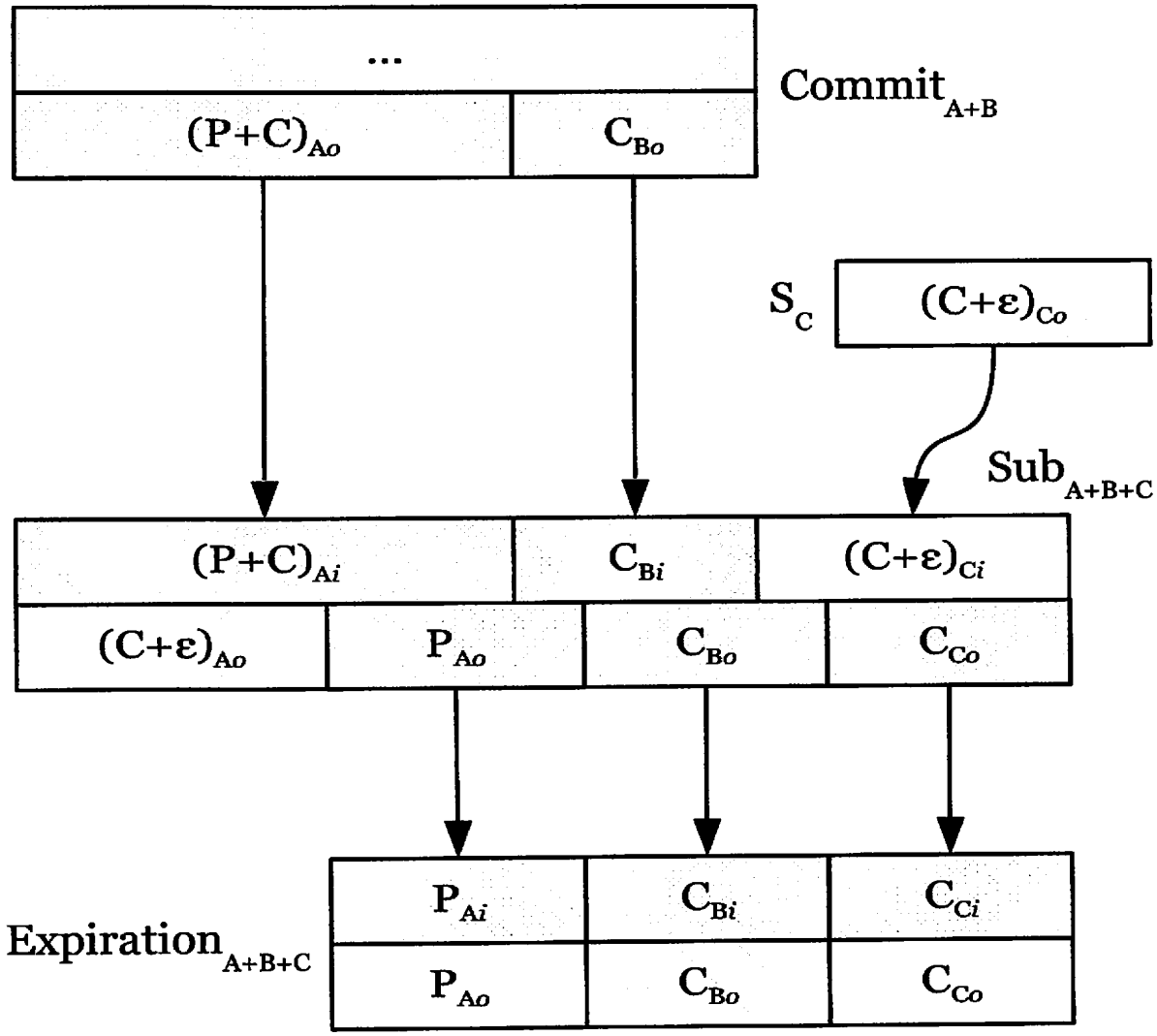


FIG. 14

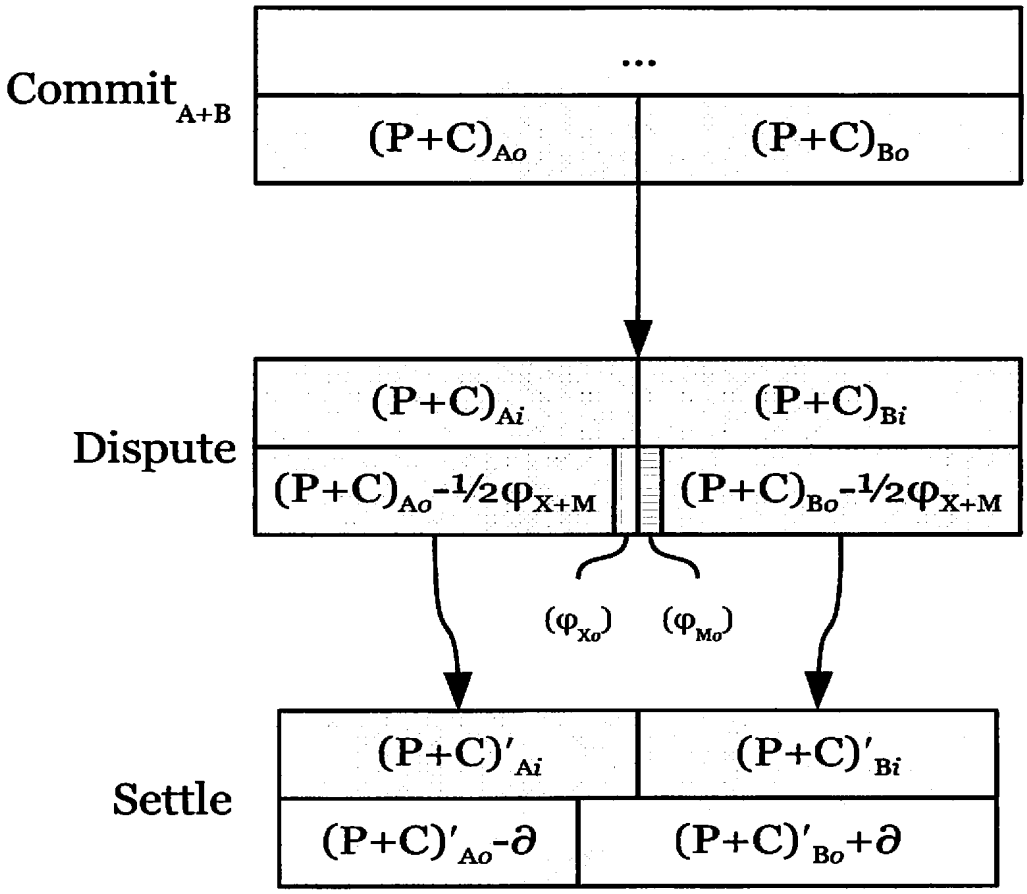

Commit A+B
...
(P+C)Ao
(P+C)Bo
Dispute
(P+C)Ai
(P+C)Bi
(P+C)Ao-½φX+M
(P+C)Bo-½φX+M
(φXo)
(φMo)
Settle
(P+C)'Ai
(P+C)'Bi
(P+C)'Ao-∂
(P+C)'Bo+∂

FIG. 15

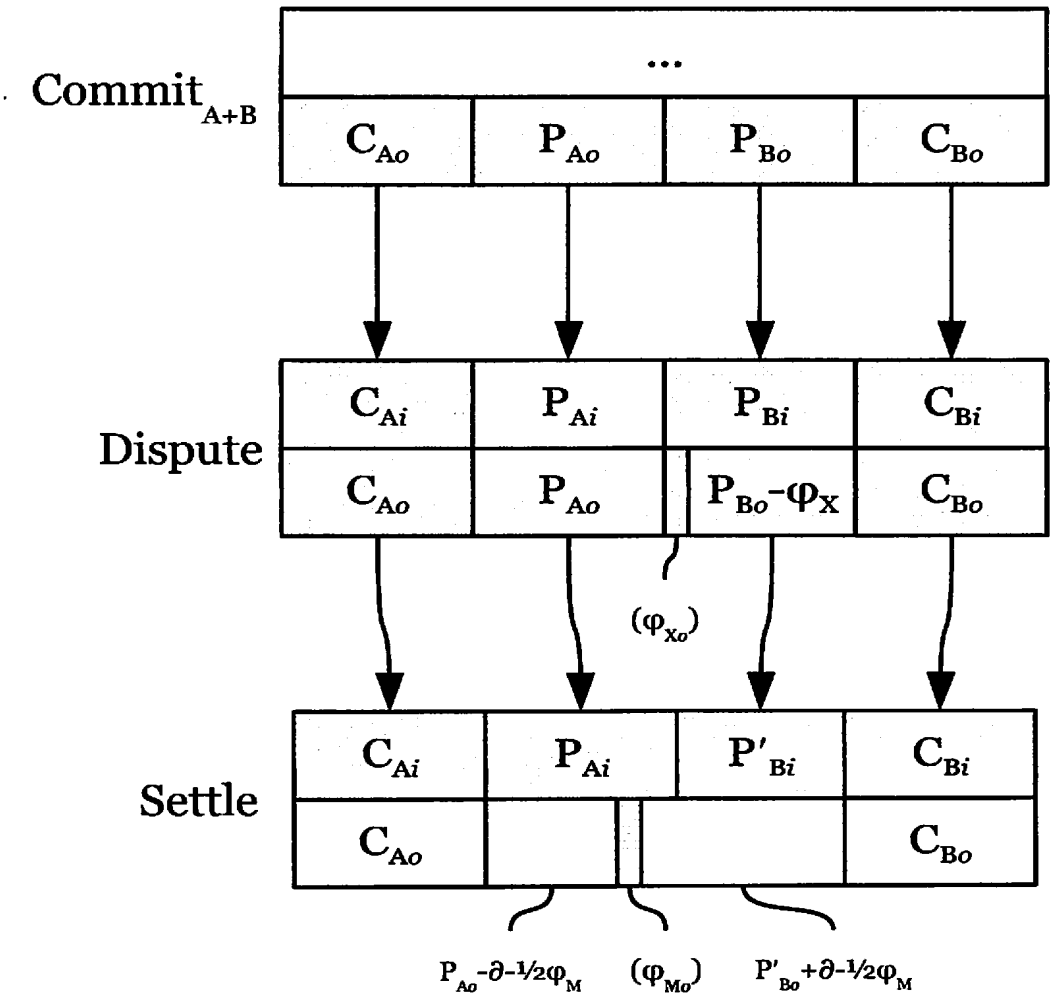

Commit A+B
...
C_{Ao}
P_{Ao}
P_{Bo}
C_{Bo}
Dispute
C_{Ai}
P_{Ai}
P_{Bi}
C_{Bi}
C_{Ao}
P_{Ao}
$P_{Bo}-\varphi_X$
C_{Bo}
(φ_{Xo})
Settle
C_{Ai}
P_{Ai}
P'_{Bi}
C_{Bi}
C_{Ao}
C_{Bo}
$P_{Ao}-\partial-\frac{1}{2}\varphi_M$
(φ_{Mo})
$P'_{Bo}+\partial-\frac{1}{2}\varphi_M$

FIG. 16

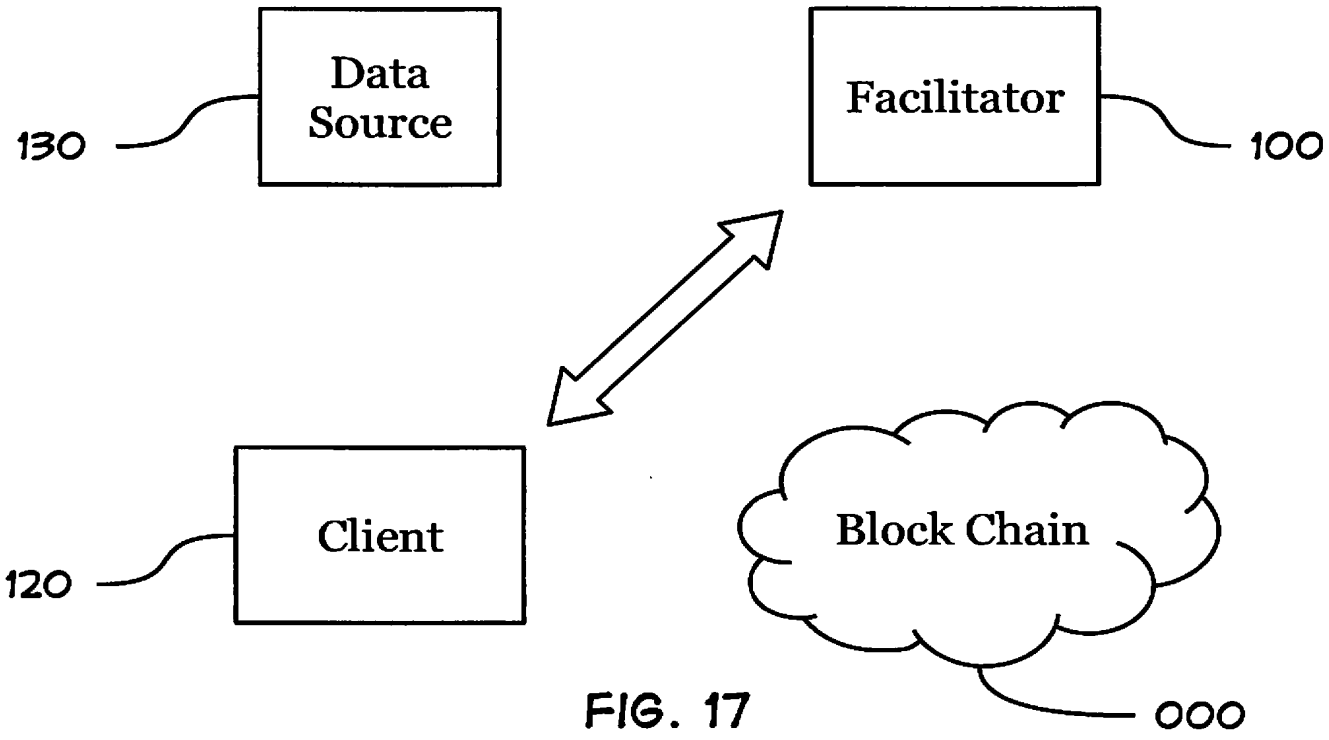

Data Source
130
Facilitator
100
Client
120
Block Chain
000

FIG. 17

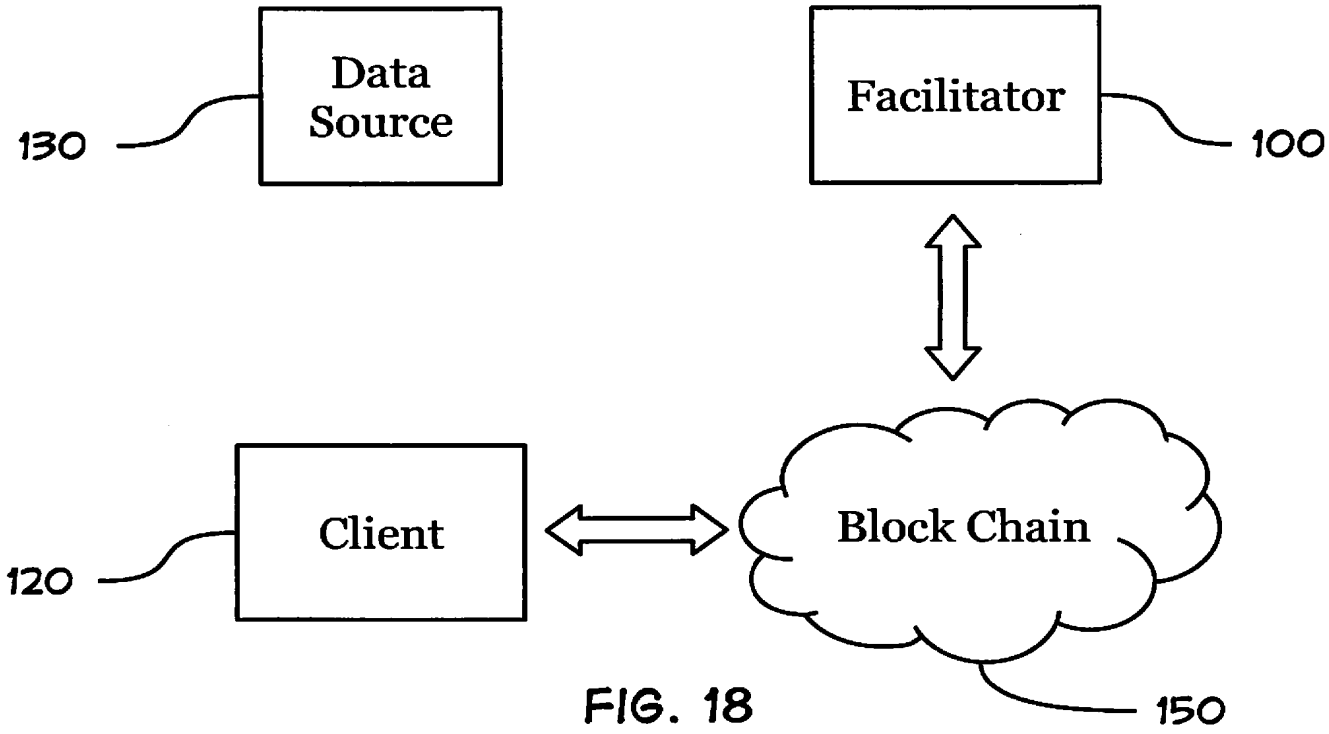

Data Source
130
Facilitator
100
Client
120
Block Chain
150

FIG. 18

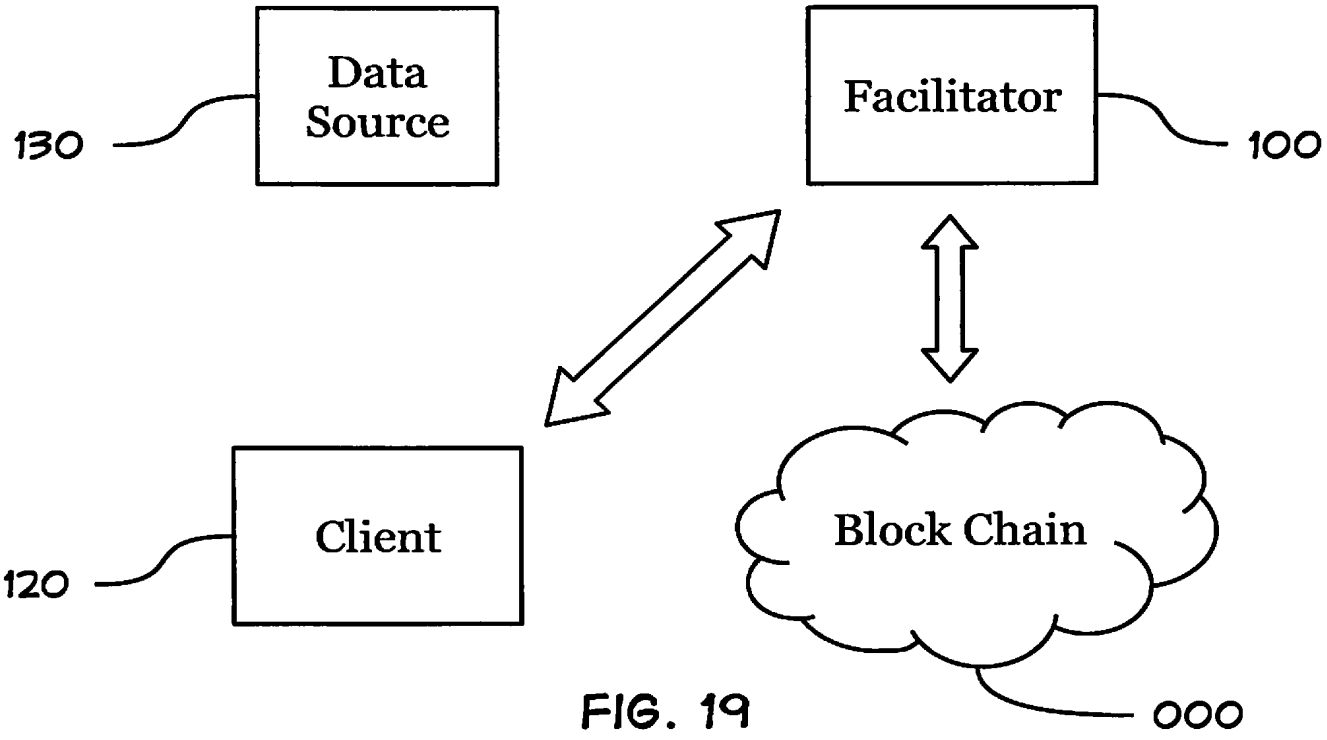

Data Source
130
Facilitator
100
Client
120
Block Chain
000

FIG. 19

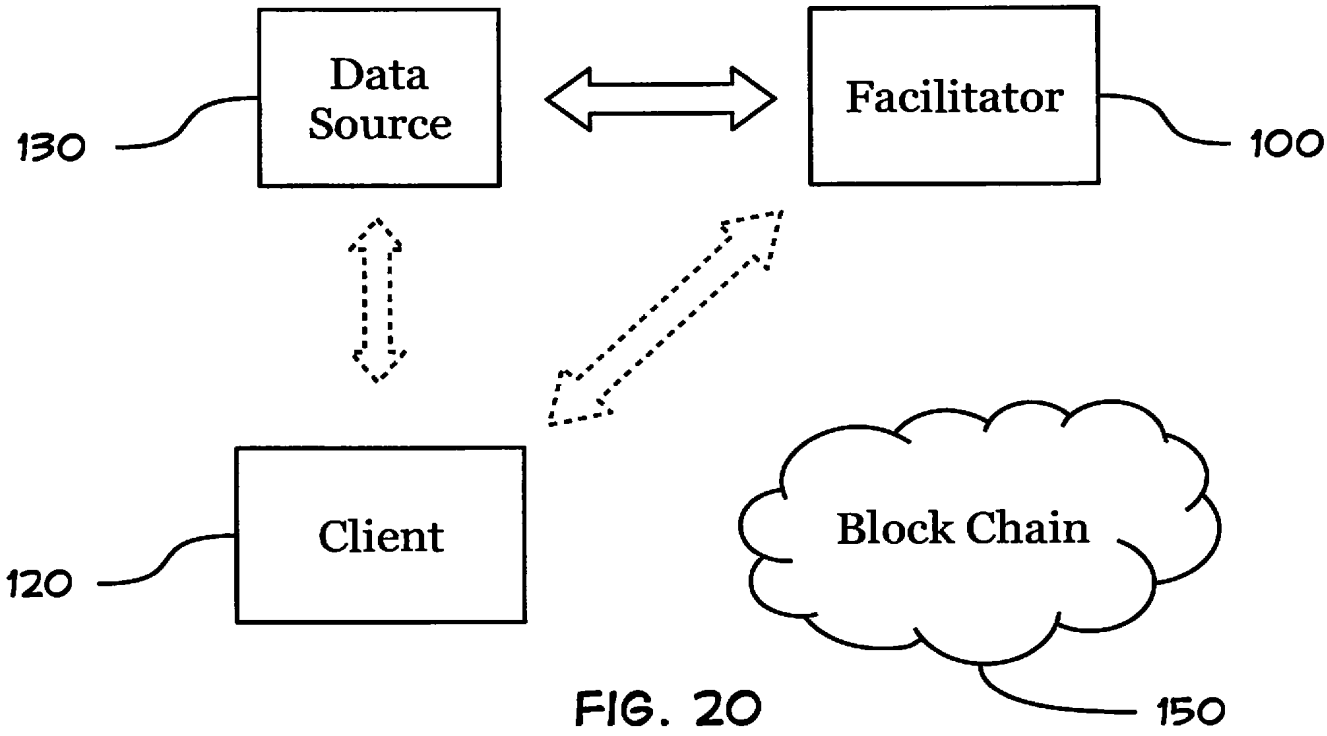

Data Source
130
Facilitator
100
Client
120
Block Chain
150

FIG. 20

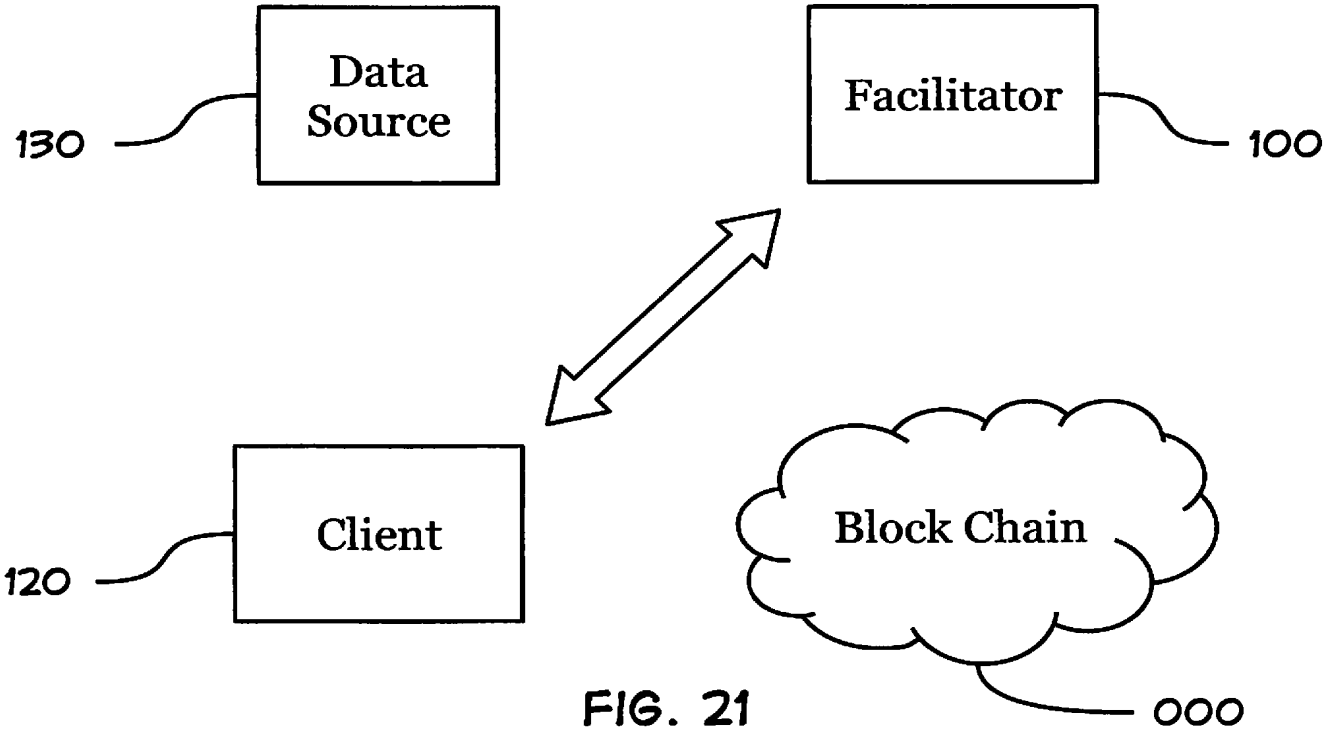

Data Source
130
Facilitator
100
Client
120
Block Chain
000

FIG. 21

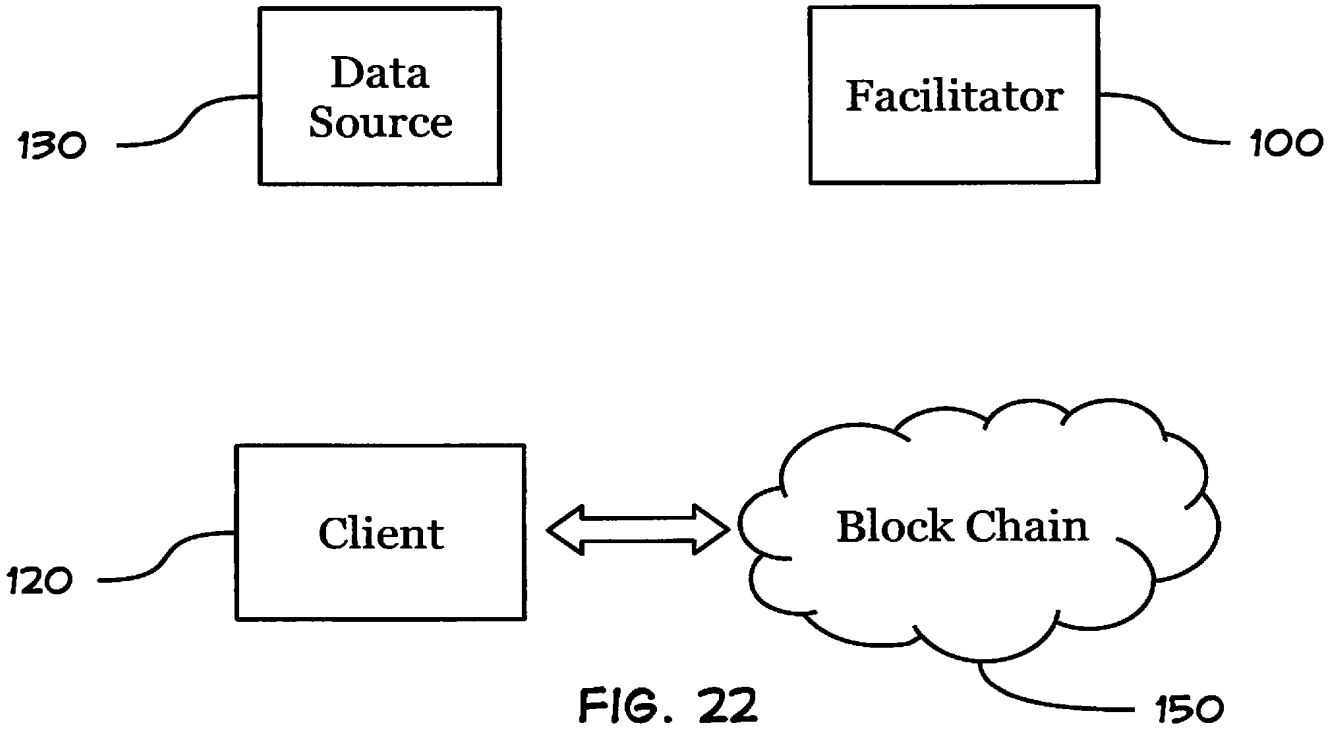

Data Source
130
Facilitator
100
Client
120
Block Chain
150

FIG. 22

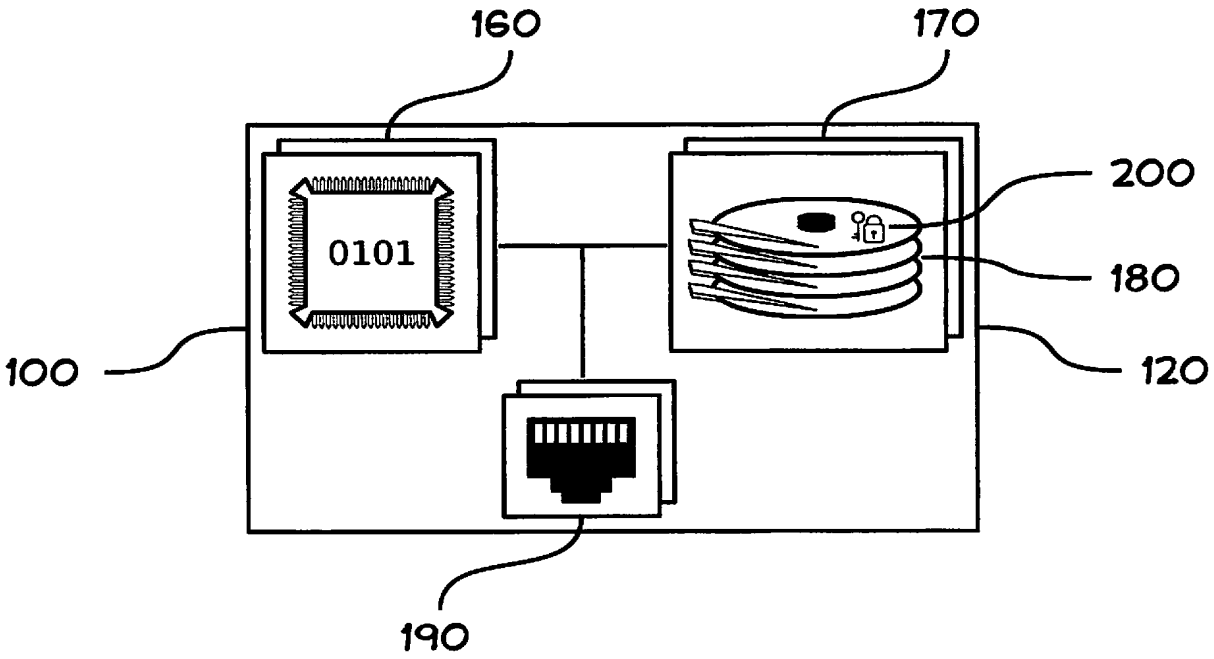


FIG. 23

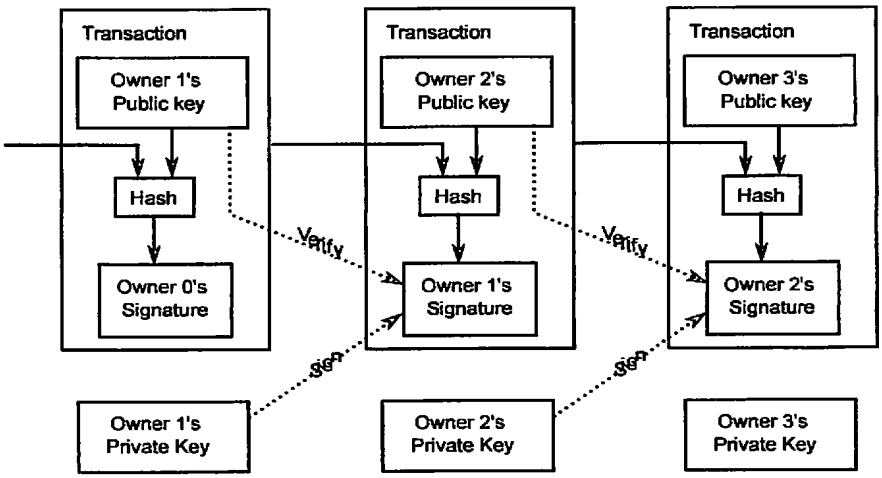


FIG. 24

(PRIOR ART)

703856

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

May 15, 2015

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE.

APPLICATION NUMBER: ***61/990,795***
FILING DATE: ***May 09, 2014***
RELATED PCT APPLICATION NUMBER: ***PCT/US15/29196***

THE COUNTRY CODE AND NUMBER OF YOUR PRIORITY APPLICATION, TO BE USED FOR FILING ABROAD UNDER THE PARIS CONVENTION, IS ***US61/990,795***

Certified by

Under Secretary of Commerce
for Intellectual Property
and Director of the United States
Patent and Trademark Office

PTO/SB/16 (03-13)
Approved for use through 01/31/2014. 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

PROVISIONAL APPLICATION FOR PATENT COVER SHEET – Page 1 of 2

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

Express Mail Label No. _____

INVENTOR(S)		
Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)
Reginald C.	Middleton	New York, NY
Matthew T.	Bogosian	Marina, CA

Additional inventors are being named on the _____ separately numbered sheets attached hereto.

TITLE OF THE INVENTION (500 characters max):

SYSTEMS AND METHODS FOR LOW TRUST AND ZERO TRUST TRANSACTIONS

Direct all correspondence to: **CORRESPONDENCE ADDRESS**

☑ The address corresponding to Customer Number: 94276

OR

☐ Firm or Individual Name

Address

City	State	Zip
Country	Telephone	Email

ENCLOSED APPLICATION PARTS (*check all that apply*)

☑ Application Data Sheet. See 37 CFR 1.76.
☐ CD(s), Number of CDs _____
☑ Drawing(s) *Number of Sheets* 12
☐ Other (specify) _____
☑ Specification (e.g., description of the invention) *Number of Pages* 60

Fees Due: Filing Fee of $260 ($130 for small entity) ($65 for micro entity). If the specification and drawings exceed 100 sheets of paper, an application size fee is also due, which is $400 ($200 for small entity) ($100 for micro entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

METHOD OF PAYMENT OF THE FILING FEE AND APPLICATION SIZE FEE FOR THIS PROVISIONAL APPLICATION FOR PATENT

☑ Applicant asserts small entity status. See 37 CFR 1.27.
☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Applicant must attach form PTO/SB/15A or B or equivalent.
☐ A check or money order made payable to the *Director of the United States Patent and Trademark Office* is enclosed to cover the filing fee and application size fee (if applicable).
☑ Payment by credit card. Form PTO-2038 is attached.
☐ The Director is hereby authorized to charge the filing fee and application size fee (if applicable) or credit any overpayment to Deposit Account Number: _____.

130
TOTAL FEE AMOUNT ($)

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. 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 10 hours 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/SB/16 (03-13)
Approved for use through 01/31/2014. 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

PROVISIONAL APPLICATION FOR PATENT COVER SHEET – Page 2 of 2

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☑ No.

☐ Yes, the invention was made by an agency of the U.S. Government. The U.S. Government agency name is: _____

☐ Yes, the invention was made under a contract with an agency of the U.S. Government. The name of the U.S. Government agency and Government contract number are: _____

WARNING:

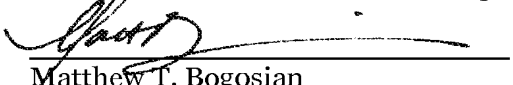
Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

SIGNATURE /Matthew T. Bogosian/ DATE May 9, 2014

TYPED OR PRINTED NAME Matthew T. Bogosian REGISTRATION NO. 69,710 (*if appropriate*)

TELEPHONE +1.831.824.4442 DOCKET NUMBER uc-lc-prov1

I hereby certify that this paper or fee is being filed with the United States Patent and Trademark Office via EFS-Web under 37 CFR § 1.8 on the Date of Deposit indicated below.

Signed: 
Name: Matthew T. Bogosian
Date of Deposit: May 9, 2014

PROVISIONAL PATENT APPLICATION

SYSTEMS AND METHODS FOR LOW TRUST AND ZERO TRUST TRANSACTIONS

COPYRIGHT STATEMENT

[1] All material in this document, including the figures, is subject to copyright protections under the laws of the United States and other countries. The owner has no objection to the reproduction of this document or its disclosure as it appears in official governmental records. All other rights are reserved.

TECHNICAL FIELD

[2] Related technical field(s) are: telecommunications, digital communications, and computer technology.

BACKGROUND ART

[3] Market efficiency tends to increase—and therefore transaction costs tend to decrease—in proportion to the degree that transacting parties trust each other. However, rent extraction tends to increase—and therefore trust decreases—in proportion to market size.[1] Efficient and productive participation in larger markets therefore requires mitigating trust issues, but that comes at a cost. That cost can often be reduced by economies of scale, but even today, there is substantial overhead from buffering against risks introduced by counterparties, intermediaries, post-delivery payment failures, guarantor failures, escrow, etc.

[4] Since the mid nineties, there has been an explosion of commercial activity where parties previously unknown to each other agree to transact using the internet as the fundamental communication medium, sometimes even across international borders. Establishing and maintaining trust between those parties has played a central role, and various crude solutions based on traditional, but inefficient methods have been attempted (e.g., electronic exchanges with expensive fees, "online" escrow and dispute resolution using third parties, various reputation systems, third party guarantors, etc.).

1 Rose, David C. The Moral Foundation of Economic Behavior. New York: Oxford UP, 2011. Print.

[5] Among those markets where individuals interact are those which trade financial instruments (e.g., stocks, bonds, options, futures, swaps, currency exposure, etc.). With the advent of financial engineering, individuals and businesses have been able to leverage computing in financial trading, including automating the process of entering and exiting trades based on programmable conditions or algorithms. However, even with the explosion of the use of technology in this space, such technology is overwhelmingly layered on top of legacy centralized markets. Nearly all impose relatively large costs to conduct trades with counterparties. Some very high-volume exchanges sell the ability for "high value" (i.e., high-paying) customers to cut in line ahead of less savvy or less well equipped investors. Some have questioned the fairness of this practice.

[6] Further, the cost of contract enforcement in international trade can be prohibitive, and success might be very difficult to predict. In addition, a seller may wish to receive one currency, and a buyer may wish to send another. The value of one currency denominated in another can be volatile. Historically, one way that remote parties have mitigated risk is to engage the assistance of trusted intermediaries. One such mechanism is a letter of credit (L/C). L/Cs are appropriate where a seller does not know whether to trust a buyer wishing to place a large order, but does trust a bank where the buyer has established a line of credit. The buyer and bank agree that the bank will release funds from that line of credit to the seller when the seller meets certain conditions (most often transmitting evidence of shipment to the bank before a certain date). The bank provides the promise (L/C) to the seller, and the seller and buyer agree on the remaining terms of the transaction. However, payment often happens at a later date than the agreement, and exchange rates could vary between the time that the agreement was struck and the time payment is received. Only the largest of institutions have the resources necessary to properly hedge against exchange rate volatility. Additionally, the fees charged by banks for L/Cs and currency exchanges are substantial. Perversely, a high degree of trust must also be placed in the intermediary institution(s), who effectively acts as self-interested document examiners who may or may not independently verify the veracity of said documents before releasing the funds, perhaps leaving much of the risk of mistake, forgery, or fraud on the shoulders of the seller. As such, L/Cs are typically not well-suited for consumer transactions, or where transactions involve currencies whose values may vary wildly in relation to each other.

[7] So-called "cryptocurrencies"—technologies that promise tightly-controlled asset creation coupled with the ability to transfer control or ownership of those assets computationally when rigorously-defined criteria are met, with little-or-no dependency on third party intermediaries,

and with very low transaction costs compared to traditional mechanisms—are relatively new creatures. The Bitcoin protocol and progeny (Ethereum, Litecoin, etc.) are one such class of technologies that have recently enjoyed meteoric rises in popularity (and valuation).

[8] For the purposes of illustration by way of example, those particular cryptocurrencies generally operate by maintaining a whole or partial history of all verified transactions. With few exceptions beyond the scope of the invention, transactions function roughly as follows.[2] A transaction comprises at least one output and at least one input. The output comprises an output "script", which comprises an ordered set of well-defined executable operations. The input comprises an input script, which comprises a second ordered set of such operations. A new (child) transaction comprises an input whose input script is combined with the output script from an existing (parent) transaction in a predictable way. Said new transaction is considered valid if others agree the combination, when evaluated, produces an anticipated state or result. A transaction output is considered "spent" if it is accepted by others as associated with a valid child transaction. A transaction output is considered "unspent" if it is not accepted as associated with any valid child transactions. The concept of "ownership" or "title" of a transaction output is determined by which entity may exercise control over said output, or, more specifically, who may create and/or expose new transactions to "spend" said output that will be accepted by others as valid.

[9] A transfer occurs when an entity produces a new child transaction that is accepted by others as valid, and whose input is associated with an output from a parent transaction. In most cases, this is a simple transfer of control to a second entity, where the new transaction's output script is a small set of operations for which creating a corresponding input script is computationally simple for a single entity in possession of a particular asymmetric cryptography key pair, and computationally impractical for all others. In other words, it is "addressed" to an entity with access to a particular private key. Existing software abstracts these addresses and simple transactions sufficiently for laypersons to engage in them without being programmers or protocol experts.

[10] However, many more complex scripts—and therefore transactions—describing conditions under which a set of asset transfers takes place are contemplated by the set of available operations. Because the general means of describing those operations is typically

2 This is an oversimplification of the Bitcoin protocol, but it is sufficient for the purposes of this disclosure. More detailed information may be found on the Bitcoin Wiki <https://en.bitcoin.it/>. Details regarding the Ethereum protocol may be found on the Ethereum Wiki <https://github.com/ethereum/wiki/wiki>.

binary or programming code[3], arbitrary transactions cannot generally be created or understood by laypersons. For example, as of April 21, 2014, the Bitcoin Contracts Wiki page comprises brief instructions for several theoretical "example" transactions.[4] In each, irrespective of role in the transaction, laypersons are unlikely able to understand—much less follow—these instructions. Fundamental steps are missing that would enable them to confidently conduct similar transactions, much less combinations of such transactions. Despite its great potential, this kind of complexity without abstraction has likely frustrated adoption of the Bitcoin protocol and progeny for anything besides "simple" payments in traditional markets.

SUMMARY OF INVENTION

[11] The invention pertains to systems and methods enabling parties with little trust or no trust in each other to enter into and enforce agreements conditioned on input from or participation of a third party, over arbitrary distances, without special technical knowledge of the underlying transfer mechanism(s), optionally affording participation of third-party mediators, substitution of transferors and transferees, term substitution, revision, or reformation, etc. Such transactions can occur reliably without involving costly third-party intermediaries who traditionally may otherwise be required for such transactions, and without traditional exposure to counterparty risk.

[12] This application explores example embodiments enabling arbitrary swaps and L/Cs. Arbitrary swaps and L/Cs are useful illustrative examples because traditionally the two are very different animals. However, the invention allows for their expression and enforcement in remarkably similar terms. As one skilled in the art will appreciate, the invention can be applied to many other agreement structures as well.

[13] In one example, Party A believes that bitcoins (BTC) will rise in notional terms when valued in New Zealand dollars (NZD) over the next few weeks. Party B believes the opposite is true, that BTC will fall when valued in NZD over a similar timeframe. Neither parties are aware of each other, but each wants to place a small bet in accordance with saidrespective beliefs. One embodiment of the invention allows those parties to discover each other, collaborate with each other to agree on concrete terms, propose transactions reflecting their agreement, and finally enforce that agreement without traditional, costly measures.

---

3 See, e.g., "bitcoind - How Can I Create a Multi Signature 2-of-3 Transaction?" StackExchange, 23 Mar. 2014. Web. 21 Apr. 2014. <https://bitcoin.stackexchange.com/questions/3712/how-can-i-create-a-multi-signature-2-of-3-transaction>.

4 Hearn, Mike. "Contracts." Bitcoin. Bitcoin Community, 9 Apr. 2014. Web. 21 Apr. 2014. <https://en.bitcoin.it/wiki/Contracts>.

[14] In another example, Party A is a merchant who wishes to allow her customers to trade their BTC for her services. However, she would rather receive US dollars (USD) because she is concerned about the volatility of BTC. Party A is not concerned about whether BTC will rise or fall when valued in USD. Periodically (e.g., once per day, hour, etc., or even once per transaction where she receives BTC), she can offer to sell exposure to BTC valued in USD in proportion to the BTC she receives from her customers. In other words, she swaps her exposure to BTC in exchange for exposure to USD. Party B has fewer BTC and more USD than he wants, and desires increased exposure to BTC valued in USD. One embodiment of the invention allows Party B to find and exchange—or "swap"—exposures with Party A, allowing Party A to accept BTC in exchange for her goods or services knowing that she will be compensated by Party B if her BTC lose value against USD, in exchange for Party B being able to keep any upside if BTC gains in value against USD. Another embodiment seeks out these swaps automatically upon detection of Party A's ownership of additional BTC.

[15] Combinations are possible. For example, Party A accepts Australian dollars (AUD), but prefers USD, and wants to hedge against volatility of AUD in USD. One embodiment of the invention allows Party A to swap exposure to USD in BTC with Party B, and simultaneously swap exposure to BTC in AUD with Party C over a similar time period, thereby synthesizing a hedge against AUD in USD. The invention is not limited such that Party B and Party C are distinct parties (they could be the same), nor is it limited such that such that Party A must conduct two separate trades. In addition, various embodiments of the invention allow the parties to perform these types of transactions without maintaining currency deposits or making currency purchases or exchanges.

[16] In yet another example, Party A wishes to purchase goods from Party B. The parties do not know each other well. Party B wants assurances of availability of funds from Party A, but Party A does not want to release those funds to Party B (or an assignee) until Party B has demonstrated proof of shipment (or met some other condition)

[17] In one embodiment comprising a swap, a first client and a second client participate in a series of transactions where assets from a first party and assets from a second party are committed until a combination of two of the first party, the second party, and an intermediary release them in accordance with a calculation by the intermediary based on observation of external state, such as the relative value of certain assets at a specific time.

[18] In another embodiment comprising an L/C, a first client and a second client participate

in a series of transactions where assets from a first party are committed until either the first client or an intermediary releases them based on observation of external state, such as verification of delivery to a shipper or an address.

[19] In a further embodiment, the assets may be refunded if no such observation can be made by an expiration time.

[20] In yet another embodiment, the commitment of assets may be extended pending a settlement facilitated by a mediator.

BRIEF DESCRIPTION OF THE DRAWINGS

[21] FIG. 1 depicts a typical embodiment for practicing the invention, especially for use with or comprising a distributed transfer mechanism, where the clients, transfer mechanism, facilitator, and oracle data source are distinct participants, and where the facilitator comprises the oracle.

[22] FIG. 2 depicts aspects of one embodiment pertaining to a swap comprising one or more source transactions and a commit transaction.

[23] FIG. 3 depicts aspects of one embodiment pertaining to a swap comprising a commit transaction and a refund transaction.

[24] FIGS. 4-5 depict aspects of swap embodiments comprising relatively simple disbursement transactions in a swap situation involving principal and collateral.

[25] FIGS. 6-7 depict transaction chains from various example swap embodiments where one party wishes to exit before termination, but cannot secure an agreement from the counterparty, but is able to find a party willing to stand in place of the party wishing to exit.

[26] FIG. 8 depicts aspects of one embodiment pertaining to an L/C comprising a source transaction and a commit transaction.

[27] FIG. 9 depicts aspects of one embodiment pertaining to an L/C comprising a commit transaction and an expiration transaction.

[28] FIGS. 10-11 depict aspects of L/C embodiments comprising relatively simple disbursement transactions in a situation involving principal and collateral.

[29] FIGS. 12-14 depict transaction chains from various example L/C embodiments

comprising substitutions of parties.

[30] FIGS. 15-16 depict aspects of embodiments where the agreeing parties have designated a mediator to resolve any dispute that may arise.

DESCRIPTION OF THE EMBODIMENTS

[31] The invention is not limited to the following embodiments. The description that follows is for purpose of illustration and not limitation. Other systems, methods, features and advantages will be or will become apparent to one skilled in the art upon examination of the figures and detailed description. It is intended that all such additional systems, methods, features, and advantages be included within this description, be within the scope of the inventive subject matter, and be protected by the accompanying Claims.

[32] For example, the Bitcoin protocol is often used in this application as an illustrative vehicle. However, the invention is not limited by the Bitcoin protocol specifically. Any technology making it sufficiently difficult to re-characterize ownership of assets (virtual or otherwise) unless certain rigorously-defined criteria are met may be substituted. The invention is not limited to decentralized or centralized transfer mechanisms. For example, in one embodiment transactions could be recognized (i.e., facilitated) by an authority (centralized). In another embodiment, they could be validated by election (distributed), etc.

[33] Further, while the Bitcoin protocol explicitly identifies "inputs" and "outputs" for transactions, the invention is not limited to such transfer mechanisms. Various embodiments of the invention may be practiced in any context in which ownership of an asset can be re-characterized, provided the transfer mechanism exposes the necessary features. This application uses "input" and "output" both literally (e.g., with respect to technologies like the Bitcoin protocol) as well figuratively (e.g., with other technologies such as those modeled after double-entry accounting, chain-of-title, etc.). In a more traditional model, for example, an "input" might comprise an amount of some or all of an available "balance" in an "account" under one entity's direction or control (e.g., at a traditional bank). An output might comprise a reference to another entity's account (e.g., an account number). In such a model, recharacterization of assets occurs when—once certain conditions are met—the balance of the first entity's account is decremented and (preferably atomically) the balance of the second entity's account is incremented. This is but one example of alternative transfer mechanisms with which the invention may be practiced.

[34] In addition, this application may disclose or imply aspects of the invention comprising a "display", an "input", a "display device", an "input device", or similar term. However, this invention is not limited to being practiced only by persons with common natural abilities. "Display [device]" is intended to comprise any device capable of unambiguously communicating information to a human being via any of the senses, or combinations of senses. For example, blind persons could use the device with an "audio display", which may comprise a text-to-speech synthesizer. Alternately, a braille terminal could be used. Similarly, "input [device]" is intended to comprise any device capable of receiving information from a human being. Modernly, popular input devices comprise a keyboard, a mouse, a touch screen, etc., but could be a speech-to-text converters, sip-and-puff devices, click-and-type devices, motion or gesture recognition devices, etc. These are but a few examples. A diversity of such display and input devices are known in the art and may be used when practicing the invention, as will become apparent to one skilled in the art.

[35] In the embodiment depicted in FIG. 1, the invention comprises some or all of the depicted participants on a computer network (not depicted). The participants comprise a first client (A) typically operated for a first party (not depicted) coupled to the computer network (either persistently or intermittently), a second client (B) typically operated for a second party (not depicted) coupled to the computer network (either persistently or intermittently), a transfer mechanism accessible via the computer network, a facilitator accessible to the computer network, optionally an oracle, and optionally an oracle data source accessible by the oracle. In a typical embodiment, the computer network comprises the internet, but this is not a requirement. Other configurations are possible. For example, multiple, independent computer networks can be used for connecting any subset of the participants, including private networks, VPNs, secure tunnels, frame relays, etc. Any computer networking technology will suffice so long as it affords communication between the various participants during times consistent with the invention.

[36] In a typical embodiment, each of the first client, the second client, and the facilitator comprises a computer processor configured to perform certain steps within the scope of the invention. In some embodiments, the oracle comprises a computer processor. In other embodiments, such as those using the Ethereum protocol as the transfer mechanism, one or both of the facilitator and the oracle comprise instructions for computation which are evaluated by participants in a proof of work protocol, in which case a participant comprises a computer processor configured to evaluate the instructions for computation. In many embodiments, a

client comprises a display device and an input device for interacting with a human being, but this is not strictly necessary. In other embodiments, a client could be fully automated, requiring no human intervention. In one such embodiment, the computer processor of the first client is configured to monitor aspects of the transfer mechanism, the facilitator, the oracle, or the second client, and is configured to interact automatically with the various participants based on an observed change of state.

[37] For example, in one embodiment, the transfer mechanism comprises the Bitcoin protocol, and each of the clients, and the facilitator comprises a non-transitory data store for storing key pairs, inchoate transactions, etc. The first client is configured such that when it observes that it acquires new ownership of BTC, it initiates an offer via the facilitator to trade exposure to one asset or asset class (e.g., BTC) in exchange for exposure to another asset or asset class (e.g., USD).

[38] FIG. 1 depicts a typical embodiment for practicing the invention—especially for use with a distributed transfer mechanism—where the clients, transfer mechanism, facilitator, and oracle data source are distinct participants, and where the facilitator comprises the oracle. However, the depicted arrangement is not the only one contemplated by the invention. In an alternate embodiment, the facilitator provides some or all aspects of the transfer mechanism. In another embodiment, the facilitator comprises some or all aspects of a client. For example, part or all of a client's data store, the ability to initiate or accept offers, etc., could be "embedded" in the facilitator, thereby enabling the facilitator to operate as a client itself (e.g., one controlled by the owners of the facilitator, or on behalf of a third party who has entrusted control to the facilitator). In yet another embodiment, the facilitator is separate and distinct from the oracle. Alternately, the oracle could comprise its own data source. Many configurations are contemplated by the invention are possible, and will become apparent to one skilled in the art.

[39] FIG. 2 depicts aspects of one embodiment pertaining to a swap comprising one or more source transactions and a commit transaction. As depicted, the commit transaction comprises a first input for accepting a first amount from a first source transaction (i.e., from a first party), a second input for accepting a second amount from a second source transaction (i.e., from a second party), and one or more outputs for directing portions of those amounts to one or more other transactions (not depicted), where the first amount and second amount total an expected amount. In many cases, the first and second amounts are equivalent, but not necessarily. In some cases the amounts comprise a principal amount (P), and (optionally) a collateral amount

(C), as depicted in the various figures.

[40] In a typical embodiment, the commit transaction is configured such that some or all of the amounts available via its output(s) may only be transferred with confirmation from at least two of the first party, the second party, the facilitator, and optionally a third party (such as a mediator). In an alternate embodiment, the commit transaction is configured such that some or all of the amounts available via its outputs may only be transferred with confirmation from one of the facilitator and optionally a trusted third party, and one of the first party and the second party. In another alternate embodiment, the commit transaction is configured such that some or all of the amounts available via its outputs may only be transferred with confirmation from either the facilitator or two of the first party, the second party, and optionally a trusted third party. These are non-limiting examples. In addition to the examples presented herein, commit transactions may be configured such that outputs vest ownership in a conjunction of any number of parties, somewhat analogous to a checking account where checks must be signed by two authorized parties in order to be honored.

[41] While a first source transaction and a second source transaction are depicted in FIG. 2, this should not be construed as a limitation of the invention. Amounts may be input into the commit transaction from any number different sources. Excesses may be refunded back to respective parties, or different parties altogether. The only limitation is that the commit transaction comprises inputs totaling at least the expected amount. In some embodiments, fees (not depicted) may be imposed for directing the amounts from their respective sources to said inputs, which may require adjusting the source transactions to compensate for those fees. For example, transfer mechanisms may impose transfer fees, withdrawal fees, wire fees, etc. The Bitcoin protocol, for example, may require a "mining fee" in order to ensure timely processing of the transfer.

[42] FIG. 3 depicts aspects of one embodiment pertaining to a swap comprising a commit transaction and a refund transaction. The commit transaction comprises a first input for receiving a first principal amount (P_A), a second input for receiving a second principal amount (P_B), and a commit output. The refund transaction comprises an input for receiving an amount from the commit output, a first refund output to the first party, and a second refund output to the second party. In a typical embodiment, the refund transaction is not created until well after the commit transaction, or created such that it is only valid after a certain time in the future and only if the commit output has not yet been spent. This allows another transaction to come before

it and spend the commit output, but if no such other transaction is created, the refund transaction can put the parties back in or close to their original positions.

[43] FIGS. 4-5 depict aspects of swap embodiments comprising relatively simple disbursement transactions in a swap situation involving principal and collateral. In FIG. 4, the commit transaction comprises a first joined principal and collateral input from a first party and a second joined principal and collateral input from a second party. In FIG. 5, the commit transaction comprises a first principal (P_A) input from a first party, a first collateral (C_A) input from the first party, a second principal (P_B) input from a second party, and a second collateral (C_B) input from the second party. These are but two of many possible configurations that will become apparent to one skilled in the art. For example, a commit transaction could comprise a principal input from a first party, a collateral input from a second party (e.g., a guarantor of the first party, not depicted), and a joined principal and collateral input from a third party.

[44] In the embodiments depicted in FIGS. 4-5, each of the disbursement transactions comprises an input for receiving an amount from the commit output. In FIG. 4, the disbursement transaction comprises a first joined modified principal and collateral disbursement output to the first party, a second joined modified principal and collateral disbursement output to the second party, and an optional fee (φ) output to a third party. In FIG. 5, the disbursement transaction comprises a collateral disbursement output to the first party, a modified principal disbursement output to the first party, a modified collateral disbursement output to the second party, and an optional fee output to a third party. Again, these are but two of many possible configurations that will become apparent to one skilled in the art. For example, analogous to above, a disbursement transaction could comprise a modified principal disbursement output to a first party, a possibly modified (if the principal was exhausted) collateral disbursement output to a third party (e.g., a guarantor of the first party), or a joined modified principal and possibly modified (if the principal was exhausted) disbursement collateral output to a second party.

[45] In each of the embodiments depicted in FIGS. 4-5, the fee is allocated from the modified principals and is shared equally among the parties to the trade, although this is not required. It could be allocated at any stage, or multiple stages. It could be born solely or disproportionately by one party. Also, in each of the embodiments depicted in FIGS. 4-5, the calculation of the amounts for two or more disbursement outputs comprises a difference (∂), which is positive to one party, and negative to another party. The disbursement transaction in the embodiment

depicted in FIG. 5 would be characteristic, for example, of a swap in which the second principal was exhausted before the expiration of the swap, thereby requiring that an amount be allocated from the collateral. In other words, where:

$$\delta > P_B - \frac{1}{2}\varphi \qquad \text{[eq. 1]}$$

[46] To illustrate by way of example how some of the various components above may be used together to facilitate various basic swap agreements, the following steps occur in one embodiment using the Bitcoin or similar protocol as the transfer mechanism, where the parties do not trust each other, and the facilitator is not fully trusted by any of the parties:

1. A first client transmits an offer to a facilitator, the offer comprising terms, the terms comprising:

    a. a reference to a base asset;

    b. a reference to a quote asset;

    c. a principal amount;

    d. an expiration time;

    e. optionally a reference to a denominating asset;

    f. optionally, a collateral amount; and

    g. optionally, a result function;

    Example terms:

        Base: USD

        Quote: AUD

        Denominating: BTC

        Principal: 0.5 (BTC)

        Collateral: 2 × principal

$res_{base}(b_o, q_o, b_f, q_f)$: $principal \times \frac{b_f - b_o}{q_f - q_o}$

Expiration: 2014-06-01T12:34:56Z

...

2. Optionally, the facilitator validates aspects of the offer (e.g., that the facilitator can interpret the terms, that the expiration time is within an acceptable range, etc.). If validation fails, the facilitator may reject the offer, optionally with an error message to the first client.

3. A second client retrieves the offer from the facilitator.

4. The first client signs a first source transaction comprising a transaction ID.

5. The second client signs a second source transaction comprising a transaction ID.

6. The second client transmits the transaction ID of the second source transaction to the first client, optionally via the facilitator, in such a way that it is associated with the offer (e.g., in the same message, via an offer ID, offer hash, etc.). In another embodiment the first client transmits the transaction ID of the first source transaction to the second client, and subsequent steps mirror the following of this embodiment.

7. One of the second client and the facilitator transmits a second public key to the first client in such a way that it is associated with the offer.

8. The first client signs a first principal input of an inchoate commit transaction for creating a complete commit transaction, the inchoate commit transaction comprising:

    a. the first principal input for receiving a first principal amount from the first source transaction;

    b. a second principal input for receiving a second principal amount from the second source transaction; and

    c. a commit output comprising a commit amount and a condition requiring signatures of private keys corresponding to two of:

        i. a first public key;

ii. the second public key; and

iii. a facilitator public key.

Example inchoate commit transaction:

```
Input:

      Previous tx: 85e5...e61f

      Index: 1

      scriptSig: efd6...ea1601 a6a6...2c2b

Input:

      Previous tx: 705d...9ce2

      Index: 0

      scriptSig: [sig. placeholder]

...

Output:

      Value: 300000000

      scriptPubKey: 2 67c1...4a70 bf9a...f9e3 cffd...1373 3
      OP_CHECKMULTISIG

...
```

9. The first client transmits the inchoate commit transaction to the second client, optionally via the facilitator. Optionally, the facilitator validates aspects of the inchoate commit transaction (e.g., that inchoate commit transaction is signed by a first party, that the first principal amount and the second principal amount each satisfy the terms, etc.). If validation fails, the facilitator may reject the inchoate commit transaction, optionally with an error message to the first client. Optionally, the facilitator transmits the offer and the inchoate commit transaction to the second client.

10. Optionally, the second client verifies that the inchoate commit transaction is as expected, signed by the first party, etc.

11. The second client creates the complete commit transaction by signing the inchoate commit transaction and optionally saves a copy in non-transitory memory, the complete commit transaction comprising:

    a. the first principal input for receiving the first principal amount from the first source transaction;

    b. a second principal input for receiving a second principal amount from the second source transaction; and

    c. a commit output comprising a commit amount and a condition requiring signatures of private keys corresponding to two of:

        i. the first public key;

        ii. the second public key; and

        iii. the facilitator public key.

Example complete commit transaction:

```
ID: 6b24...b607

Input:

      Previous tx: 85e5...e61f

      Index: 1

      scriptSig: efd6...ea1601 a6a6...2c2b

Input:

      Previous tx: 705d...9ce2

      Index: 0

      scriptSig: 78eb...fc4501 531f...00dd
```

```
...

Output:

    Value: 300000000

    scriptPubKey: 2 67c1...4a70 bf9a...f9e3 cffd...1373 3
    OP_CHECKMULTISIG

...
```

12. The second client signs an inchoate refund transaction comprising:

    a. a lock time after the expiration time;

    b. an input for receiving the commit amount from the complete commit transaction;

    c. a first refund output comprising a first refund amount and a first condition requiring approval of the first party; and

    d. a second refund output comprising a second refund amount and a condition requiring approval of a second party.

Example inchoate refund transaction:

```
Input:

    Previous tx: 6b24...b607

    Index: 0

    scriptSig: OP_0 [sig. placeholder] c255...d80301

Output:

    Value: 149995000

    scriptPubKey: OP_DUP OP_HASH160 53a5...8974
    OP_EQUALVERIFY OP_CHECKSIG

Output:
```

```
            Value: 149995000

            scriptPubKey: OP_DUP OP_HASH160 30e6...2511
            OP_EQUALVERIFY OP_CHECKSIG

        ...

        nLockTime: 2014-06-03T12:34:56Z
```

13. The second client transmits the complete commit transaction and the inchoate refund transaction to the to the first client, optionally via the facilitator. Optionally, the facilitator validates aspects of the complete commit transaction and the inchoate refund transaction (e.g., that complete refund transaction is signed by the first party and the second party, that inchoate refund transaction is signed by the second party, that aspects of the complete commit transaction match the inchoate commit transaction, that the first refund amount of the signed complete refund transaction is not more than the first principal amount, that the second refund amount of the signed complete refund transaction is not more than the second principal amount, that the lock time is after the expiration time, etc.). If validation fails, the facilitator may reject the inchoate refund transaction or the complete commit transaction, optionally with an error message to the second client. Optionally, the facilitator transmits the complete commit transaction and the inchoate refund transaction to the first client.

14. Optionally, the first client verifies that the complete commit transaction is as expected and signed by the first party and the second party, that the inchoate refund transaction is as expected and is signed by the second party, etc.

15. Optionally, the first client saves a copy of the complete commit transaction in non-transitory memory.

16. The first client creates the complete refund transaction and saves a copy in non-transitory memory, the complete refund transaction comprising:

    a. a lock time after the expiration time;

    b. an input for receiving the commit amount from the complete commit transaction;

    c. a first refund output comprising a first refund amount and a first condition

requiring approval of the first party; and

a second refund output comprising a second refund amount and a condition requiring approval of the second party.

Example complete refund transaction:

```
ID: d5f8...8ab5

Input:

      Previous tx: 6b24...b607

      Index: 0

      scriptSig: OP_0 b859...452c01 c255...d80301

Output:

      Value: 149995000

      scriptPubKey: OP_DUP OP_HASH160 53a5...8974
      OP_EQUALVERIFY OP_CHECKSIG

Output:

      Value: 149995000

      scriptPubKey: OP_DUP OP_HASH160 30e6...2511
      OP_EQUALVERIFY OP_CHECKSIG

...

nLockTime: 2014-06-03T12:34:56Z
```

17. The first client transmits the complete refund transaction to the second client, optionally via the facilitator. Optionally, the facilitator validates aspects of the complete refund transaction (e.g., that complete refund transaction is signed by both the first party, that the complete refund transaction has not otherwise been modified, is consistent with the terms and the complete commit transaction, etc.). If validation fails, the facilitator may reject the complete refund transaction, optionally with an error message to the first

client. Optionally, the facilitator transmits the complete refund transaction to the second client.

18. Optionally, the second client verifies that the complete refund transaction is as expected and signed by the first party and the second party, etc.

19. After creating or receiving both the complete commit transaction and the complete refund transaction, the first client broadcasts the first source transaction.

20. After creating or receiving both the complete commit transaction and the complete refund transaction, the second client broadcasts the second source transaction.

21. After seeing that both the first source transaction and second source transaction have been broadcast, one or both of the first client the second client broadcast the complete commit transaction.

22. On or after the expiration time or at a time or upon an event as defined by the terms, and before the lock time of the complete refund transaction, the facilitator performs a calculation in accordance with the terms for determining a first disbursement amount and a second disbursement amount, optionally requesting information from an oracle for use in the calculation (e.g., the most recent price of an asset pair, the price of the asset pair at the time the offer was accepted, etc.). In one embodiment, the facilitator queries an oracle, which comprises a data source that could comprise an external data feed, internal database, another oracle, etc.

In the example embodiment, given a time t, the oracle provides the value at t of one or more of: the base asset, the quote asset, the base asset in terms of the denominating asset b_t, the quote asset in terms of the denominating asset q_t, or the base asset in terms of the quote asset (e.g., if the base asset or the quote asset is also the denominating asset).

In continuing the example above, the base asset is USD, the quote asset is AUD, and the denominating asset is BTC. b_o is the value of USD in BTC at the time the trade is initiated. b_f is the value of USD in BTC at the time the trade is completed. q_o is the value of AUD in BTC at the time the trade is initiated. q_f is the value of AUD in BTC at the time the trade is completed. The calculation the facilitator uses to compute the first disbursement amount and the second disbursement amount comprises $res_{base}(b_o, q_o, b_f,$

q_f). In typical embodiments, a party's loss is proportionate to its counterparty's gain, implying:

$$res_{quote}(b_{o,} q_{o,} b_f, q_f) \quad = \quad -res_{base}(b_{o,} q_{o,} b_f, q_f) \qquad \text{[eq. 2]}$$

23. The facilitator signs an inchoate disbursement transaction, which comprises:

a. an input for receiving the commit amount from the complete commit transaction;

b. a first disbursement output comprising the first disbursement amount and a first condition requiring approval of the first party;

c. a second disbursement output comprising the second disbursement amount and a condition requiring approval of the second party; and

d. optionally a third disbursement output comprising a fee amount and a condition requiring approval of a third party;

typically where the sum of the first disbursement amount, the second disbursement amount, and any fee amount is not more than the commit amount from the complete commit transaction.

Example inchoate disbursement transaction:

```
Input:

     Previous tx: 6b24...b607

     Index: 0

     scriptSig: OP_0 [sig. placeholder] ddbb...b00601

Output:

     Value: 142500736

     scriptPubKey: OP_DUP OP_HASH160 53a5...8974
     OP_EQUALVERIFY OP_CHECKSIG

Output:
```

```
        Value: 157479264

        scriptPubKey: OP_DUP OP_HASH160 30e6...2511
        OP_EQUALVERIFY OP_CHECKSIG

    Output:

        Value: 10000

        scriptPubKey: OP_DUP OP_HASH160 d377...5c8c
        OP_EQUALVERIFY OP_CHECKSIG

    ...
```

24. The facilitator transmits the inchoate disbursement transaction to both the first client and the second client, either of whom may independently verify, sign, and broadcast the disbursement transaction before the time arrives that the other can successfully broadcast the complete refund transaction.

[47] The above is but one embodiment of a transaction according to the invention. In another, equivalent or alternate steps may be used. The following describes an embodiment comprising an atypical, but illustrative arrangement:

1. A first client transmits an offer to a second client.

2. The first client transmits the offer to a facilitator.

3. The facilitator transmits to the first client a first inchoate commit transaction for creating a complete commit transaction, the first inchoate commit transaction comprising:

    a. a first principal input for receiving a first principal amount from a first source transaction; and

    b. a first commit output comprising a first commit amount and a condition requiring approval of two of:

        i. a first party;

        ii. a second party; and

        iii. the facilitator.

4. The facilitator transmits to the second client a second inchoate commit transaction for creating a complete commit transaction, the second inchoate commit transaction comprising:

    a. a second principal input for receiving a second principal amount from a second source transaction; and

    b. a second commit output comprising a second commit amount and a condition requiring approval of two of:

        i. the first party;

        ii. the second party; and

        iii. the facilitator.

5. The first clint signs the first source transaction.

6. The first client completes and signs (e.g., with `SIGHASH_SINGLE | SIGHASH_ANYONECANPAY`) the first inchoate commit transaction.

    Example first inchoate commit transaction:

```
...
Input:
      Previous tx: 85e5...e61f
      Index: 1
      scriptSig: 5e7c...a11a83 ecad...d0ba
...
Output:
      Value: 150000000
      scriptPubKey: 2 67c1...4a70 bf9a...f9e3 cffd...1373 3
      OP_CHECKMULTISIG
```

...

7. The first client transmits the first inchoate commit transaction to the facilitator.

8. The second clint signs the second source transaction.

9. The second client completes and signs (e.g., with `SIGHASH_SINGLE | SIGHASH_ANYONECANPAY`) the second inchoate commit transaction.

   Example second inchoate commit transaction:

```
...
Input:
    Previous tx: 705d...9ce2
    Index: 0
    scriptSig: ade1...9dcb83 f058...878a
...
Output:
    Value: 150000000
    scriptPubKey: 2 67c1...4a70 bf9a...f9e3 cffd...1373 3
    OP_CHECKMULTISIG
...
```

10. The second client transmits the second inchoate commit transaction to the facilitator.

11. The facilitator creates the complete commit transaction from the first inchoate transaction and the second inchoate commit transaction, the complete commit transaction comprising:

    a. a first principal input for receiving a first principal amount from the first source transaction; and

    b. a first commit output comprising a first commit amount and a condition

requiring approval of two of:

i. the first party;

ii. the second party; and

iii. the facilitator;

c. a second principal input for receiving a second principal amount from the first source transaction; and

d. a second commit output comprising a second commit amount and a condition requiring approval of two of:

i. the first party;

ii. the second party; and

iii. the facilitator.

Example complete commit transaction:

```
ID: 11f0...8ea8

Input:

      Previous tx: 85e5...e61f

      Index: 1

      scriptSig: 5e7c...a11a83 ecad...d0ba

Input:

      Previous tx: 705d...9ce2

      Index: 0

      scriptSig: ade1...9dcb83 f058...878a

...

Output:
```

```
        Value: 150000000

        scriptPubKey: 2 67c1...4a70 bf9a...f9e3 cffd...1373 3
        OP_CHECKMULTISIG

    Output:

        Value: 150000000

        scriptPubKey: 2 67c1...4a70 bf9a...f9e3 cffd...1373 3
        OP_CHECKMULTISIG

    ...
```

In another embodiment, the first client provides a transaction ID of the first source transaction to the facilitator and the second client provides a transaction ID of the second source transaction to the facilitator before the facilitator transmits the first inchoate commit transaction and the second inchoate commit transaction. The facilitator creates the first inchoate commit transaction identical to the second inchoate commit transaction, each comprising a first principal input with a placeholder signature and a second principal input with a placeholder signature. Once the respective inchoate commit transactions are transmitted to the respective clients, the clients each sign their respective principal input (e.g., with `SIGHASH_ALL | SIGHASH_ANYONECANPAY`) before returning their respective signed inchoate commit transaction back to the facilitator. The facilitator collects the signed inchoate commit transactions and consolidates the signed inputs into a complete commit transaction. In such an embodiment, the first commit output and the second commit output could be consolidated, and the corresponding disbursement transaction and refund transaction could omit their respective second inputs.

12. The facilitator transmits the completed commit transaction to the first client who optionally stores it in non-transitory memory.

13. The facilitator transmits the completed commit transaction to the second client who optionally stores it in non-transitory memory.

14. The first client signs (e.g., `SIGHASH_ALL | SIGHASH_ANYONECANPAY` or `SIGHASH_SINGLE | SIGHASH_ANYONECANPAY`) an inchoate refund transaction

comprising:

a. a lock time after the expiration time;

b. a first input for receiving the first commit amount from the complete commit transaction;

c. a second input for receiving the second commit amount from the complete commit transaction;

d. a first refund output comprising a first refund amount and a first condition requiring approval of the first party; and

e. a second refund output comprising a second refund amount and a second condition requiring approval of the second party.

Example inchoate refund transaction:

```
Input:
     Previous tx: 11f0...8ea8
     Index: 0
     scriptSig: OP_0 78a2...203181 [sig. placeholder]
Input:
     Previous tx: 11f0...8ea8
     Index: 1
     scriptSig: OP_0 fdbe...893f81 [sig. placeholder]
...
Output:
     Value: 149995000
     scriptPubKey: OP_DUP OP_HASH160 53a5...8974
     OP_EQUALVERIFY OP_CHECKSIG
```

Output:

Value: **149995000**

scriptPubKey: **OP_DUP OP_HASH160 30e6...2511 OP_EQUALVERIFY OP_CHECKSIG**

...

nLockTime: **2014-06-03T12:34:56Z**

15. The first client transmits the complete commit transaction and the inchoate refund transaction to the second client.

16. The second client creates the complete refund transaction from the inchoate refund transaction (e.g., signing with `SIGHASH_ALL | SIGHASH_ANYONECANPAY` or `SIGHASH_SINGLE | SIGHASH_ANYONECANPAY`) and saves a copy in non-transitory memory.

Example complete refund transaction:

ID: **eb09...3d15**

Input:

Previous tx: 11f0...8ea8

Index: 0

scriptSig: OP_0 78a2...203181 **b765...fc4383**

Input:

Previous tx: 11f0...8ea8

Index: 1

scriptSig: OP_0 fdbe...893f81 **91e4...4dd583**

...

Output:

```
        Value: 149995000

        scriptPubKey: OP_DUP OP_HASH160 53a5...8974
        OP_EQUALVERIFY OP_CHECKSIG

    Output:

        Value: 149995000

        scriptPubKey: OP_DUP OP_HASH160 30e6...2511
        OP_EQUALVERIFY OP_CHECKSIG

    ...

    nLockTime: 2014-06-03T12:34:56Z
```

17. The second client transmits the complete refund transaction to the first client.

18. After creating or receiving both the complete commit transaction and the complete refund transaction, the first client broadcasts the first source transaction.

19. After creating or receiving both the complete commit transaction and the complete refund transaction, the second client broadcasts the second source transaction.

20. After seeing that both the first source transaction and second source transaction have been broadcast, one or both of the first client the second client broadcast the complete commit transaction.

21. On or after the expiration time, or at a time or upon an event as defined by the terms, and before the lock time of the complete refund transaction, the facilitator performs a calculation in accordance with the terms for determining a first disbursement amount and a second disbursement amount, optionally requesting information from an oracle for use in the calculation.

22. The facilitator signs a disbursement transaction (e.g., signing with `SIGHASH_ALL | SIGHASH_ANYONECANPAY` or `SIGHASH_SINGLE | SIGHASH_ANYONECANPAY`).

    Example inchoate disbursement transaction:

```
    Input:
```

```
        Previous tx: 11f0...8ea8

        Index: 0

        scriptSig: OP_0 [sig. placeholder] 8cd3...d86481

    Input:

        Previous tx: 11f0...8ea8

        Index: 1

        scriptSig: OP_0 [sig. placeholder] 12bc...825281

    ...

    Output:

        Value: 142500736

        scriptPubKey: OP_DUP OP_HASH160 53a5...8974
        OP_EQUALVERIFY OP_CHECKSIG

    Output:

        Value: 157479264

        scriptPubKey: OP_DUP OP_HASH160 30e6...2511
        OP_EQUALVERIFY OP_CHECKSIG

    Output:

        Value: 10000

        scriptPubKey: OP_DUP OP_HASH160 d377...5c8c
        OP_EQUALVERIFY OP_CHECKSIG

    ...
```

23. The facilitator transmits the inchoate disbursement transaction to both the first client and the second client, either of whom can broadcast it as in the prior example embodiment.

[48] Various verification steps have been omitted for brevity.

[49] It will become apparent to one skilled in the art that aspects of each of embodiments above may be comingled. For example, the first client could transmit the offer to the facilitator, where the second client could find and retrieve it. As mentioned above, aspects of one or both of the first client and the second client could coincide with the facilitator allowing many of the above steps to be omitted as redundant where the facilitator is entrusted to act as a proxy for or on behalf of one of the first party and the second party. The facilitator could contain aspects of one of the clients, but not the other, in which case the extra-facilitator client would optionally independently validate transactions it received from the facilitator before signing them, etc. In such embodiments, the facilitator typically comprises a means to control aspects of a client it comprises via an interface such as a web-based user interface (UI), an application programmer's interface (API), etc.

[50] In such embodiments, any party delegating authority to the facilitator must trust the facilitator to be secure and to act fairly, but these are similar to expectations many parties already have of traditional third party intermediaries. Assuming the first party has independent access to same key pairs the facilitator uses to act on behalf of the first party, and the second party has independent access to the same key pairs the facilitator uses to act on behalf of the second party, even if the facilitator is destroyed, both the first party and the second party may retrieve their assets, at worst by broadcasting any signed refund transaction on or after the lock time, assuming they have kept copies of the signed refund transaction in their respective non-transitory memories.

[51] In one embodiment, a client is configured such that when it detects a new spendable output comprising an amount (e.g., by monitoring changes in the blockchain when using the Bitcoin or similar protocol as the transfer mechanism), it automatically accepts a remote offer comprising an amount compatible with the amount of the new spendable output. If no such remote offer is available, it transmits an offer comprising an amount substantially similar to the new spendable output (e.g., to the facilitator, to another client, etc.). In another embodiment, when the client detects a second new spendable output, it attempts to rescind the offer. If successful, it transmits a new offer comprising an amount which comprises some or all of the new spendable output and some or all of the second new spendable output. Other variations are possible. For example, the client is configured to scan available offers and match the available offers to the amounts of the spendable outputs. Matching algorithms vary in complexity and are

known in the art. For example, many Bitcoin protocol client implementations provide such algorithms for matching spendable outputs to the inputs of simple transactions. Such algorithms are adaptable by those of ordinary skill in the art for this and similar embodiments of the invention.

[52] In various embodiments, the terms comprise a ratio of a first asset to a second asset, optionally denominated in a third asset, as well as an amount that each participant must allocate. For example, in one embodiment, the terms could offer to "sell" 2 BTC/USD with a required allocation of 3 BTC from each party. In other words, the swap defined by the terms offers exposure to 2 BTC of USD, and each participant must allocate 2 BTC to principal and 1 BTC to collateral for the duration of the swap (i.e., until it expires, or until the principal and collateral of one party is exhausted).

[53] The allocations for each party need not be equal. In one embodiment, if the market expects a particular asset pair to decline over the life of the swap, the party accepting exposure to that asset may be required to allocate more collateral than the counterparty. Note that in the previous example, the parties' risk formulas are asymmetric. The most the offeror could lose is the principal of 2 BTC (if BTC become worthless when valued in USD). However, the offeree's losses are unbounded (if USD becomes worthless when valued in BTC). In other words:

$$res_{base}(b_{o,} q_{o,} b_f, q_f) \quad = \quad principal \times \frac{b_f - b_o}{q_f - q_o} \qquad \text{[eq. 3]}$$

[54] Alternately:

$$res_{base}(b_{o,} q_{o,} b_f, q_f) \quad = \quad principal \times \left(\frac{b_f}{q_f} - \frac{b_o}{q_o} \right) \qquad \text{[eq. 4]}$$

[55] In other embodiments symmetrical models could be adopted. Consider:

$$res_{base}(b_{o,} q_{o,} b_f, q_f) \quad = \quad \begin{cases} \frac{b_t}{q_f} \leq \frac{b_o}{q_o} & : \quad principal \times \left(\frac{b_f q_o}{b_o q_f} - 1 \right) \\ \frac{b_t}{q_f} > \frac{b_o}{q_o} & : \quad principal \times \left(1 - \frac{b_o q_f}{b_f q_o} \right) \end{cases} \qquad \text{[eq. 5]}$$

[56] Where $res_{base}(...)$ is the resulting gain or loss to the party taking the base asset exposure

at time f given the initial value of the base asset b_0, the initial value of the quote asset q_0, the value of the base asset b_f at time f, and the value of the quote asset q_f at time f. The resulting gain or loss for the party taking the quote asset exposure is inverted:

$$\begin{aligned} res_{quote}(b_0, q_0, b_f, q_f) &= -res_{base}(b_0, q_0, b_f, q_f) \\ &= \begin{cases} \frac{b_f}{q_f} \leq \frac{b_0}{q_0} & : \quad principal \times \left(1 - \frac{b_f q_0}{b_0 q_f}\right) \\ \frac{b_f}{q_f} > \frac{b_0}{q_0} & : \quad principal \times \left(\frac{b_0 q_f}{b_f q_0} - 1\right) \end{cases} \end{aligned} \qquad \text{[eq. 6]}$$

[57] In this embodiment, the parties' risk formulas are symmetric. If the base asset goes to zero, the most the party taking the base asset exposure can lose is the principal. Likewise, if the quote asset goes to zero, the most the party taking the quote asset exposure can lose is the principal. Note that no collateral is needed. Alternately, consider:

$$\begin{aligned} res_{base}(b_0, q_0, b_f, q_f) &= -res_{quote}(b_0, q_0, b_f, q_f) \\ &= \begin{cases} \frac{b_f}{q_f} \leq \frac{b_0}{q_0} & : \quad -principal \times \frac{b_0 q_f}{b_f q_0} \\ \frac{b_f}{q_f} > \frac{b_0}{q_0} & : \quad principal \times \frac{b_f q_0}{b_0 q_f} \end{cases} \end{aligned} \qquad \text{[eq. 7]}$$

[58] In this embodiment, the parties' risk formulas are also symmetric. However, as the base asset goes to zero, the loss incurred by the party taking the base asset approaches infinity, all else being equal. Likewise, as the quote asset goes to zero, the loss incurred by the party taking the quote asset position approaches infinity, all else being equal. Note that collateral is needed when losses exceed principal amounts. The more volatile the asset pair, the more collateral may be required to minimize risk of termination before expiration. These are but a few basic examples. Terms affecting the calculation for determining the allocation disbursement amounts can be arbitrarily complex and are limited by the imaginations of the participants. All such variations are contemplated by the invention.

[59] In some circumstances, a party may wish to exit a swap before it terminates. The parties may agree to terminate prematurely. In one embodiment, the facilitator facilitates this by creating the unsigned disbursement transaction as if the swap was terminated when the parties agreed to exit. The requesting party signs the unsigned disbursement transaction and transmits

it to the acquiescing party who signs and broadcasts it. Optionally, if the facilitator includes a fee output to a third party, the acquiescing party may require that the fee would be born disproportionately, or entirely by the requesting party.

[60] Where one party wishes to exit before termination, but cannot secure an agreement from the counterparty, another option is for the party seeking premature termination to find a third party substitute. FIGS. 6-7 depict transaction chains from various example swap embodiments comprising such substitutions.

[61] FIG. 6 depicts aspects of an embodiment where a withdrawing party (A) has convinced an entering party (C) to substitute into a transaction with a remaining party (B). In addition, the entering party transfers a negotiated amount (ε) to the withdrawing party. This is facilitated in the depicted embodiment by a substitution transaction, a second commit transaction, and a second refund transaction.

[62] For clarity of illustration, the outputs of the commit transaction and the corresponding inputs of the substitution transaction are depicted as separate for each of the first principal (P_A), the first collateral (C_A), the second principal (P_B), and the second collateral (C_B). This is not a limitation of the invention. Just as with the previously described embodiments, the outputs of the commit transaction, and corresponding inputs of the substitution transaction could be any configuration considered valid by the transfer mechanism. The outputs of the substitution transaction and inputs to the second commit transaction are similarly depicted for clarity of illustration. Again, all valid configurations of inputs and outputs between transactions are contemplated by the invention.

[63] A difference (∂) used to calculate the first disbursement amount and the second disbursement amount as if the transaction had been terminated at the time of the substitution. In the embodiment depicted in FIG. 6, this favors the remaining party. Therefore, the substitution transaction is constructed such that the withdrawing party takes a loss in proportion to that difference, and the entering party need only provide assets to cover the remaining position.

[64] Also, in the embodiment depicted in FIG. 6, the substitute refund is asymmetric. The entering party is refunded what that party committed to the transaction (less the negotiated amount), and the remaining party is refunded what that party would have received had the swap been terminated at the time of substitution. Other variations are possible. For example, in one

embodiment, the negotiated amount may be transferred separately, or at another phase of the swap.

[65] In the embodiment depicted in FIG. 7, the substitution favors the withdrawing party. In that embodiment, the substitute refund is symmetric. The remaining party is refunded what that party would have received had the original transaction been refunded.

[66] In one embodiment, a substitution is facilitated by the following steps:

1. The facilitator performs a calculation in accordance with the terms for determining a withdrawal amount and an entry amount, optionally requesting information from an oracle for use in the calculation.

2. The facilitator creates an inchoate substitution transaction comprising:

    a. a first input for receiving an amount from a commit transaction;

    b. an entry input for receiving the entry amount from a source transaction;

    c. a withdrawal output comprising the withdrawal amount and a first condition requiring approval of the first party; and

    d. a substitution output comprising a substitution amount and a second condition requiring approval of two of:

        i. the second party;

        ii. the third party; and

        iii. the facilitator.

    Example substitution transaction:

```
Input:

    Previous tx: 6b24...b607

    Index: 0

    scriptSig: OP_0 [sig. placeholder] [sig. placeholder]
```

```
Input:
        Previous tx: dd66...ae8e
        Index: 3
        scriptSig: [sig. placeholder]
Output:
        Value: 300000000
        scriptPubKey: 2 bf9a...f9e3 952b...0542 cffd...1373 3
        OP_CHECKMULTISIG
Output:
        Value: 121871000
        scriptPubKey: OP_DUP OP_HASH160 6250...6cfc
        OP_EQUALVERIFY OP_CHECKSIG
...
```

3. The facilitator transmits the inchoate substitution transaction to the first party and the third party.

4. The first party signs the first input of inchoate substitution transaction (e.g., signing with `SIGHASH_ALL | SIGHASH_ANYONECANPAY`) and transmits the first signed inchoate substitution transaction to the facilitator.

5. The third party signs the entry input of the inchoate substitution transaction (e.g., signing with `SIGHASH_ALL | SIGHASH_ANYONECANPAY`) and transmits the second signed inchoate substitution transaction to the facilitator.

6. The facilitator creates a complete substitution transaction (e.g., `ID: 9c8b...4794`) from the first inchoate substitution transaction and the second inchoate substitution transaction.

7. The facilitator signs an inchoate substitute refund transaction comprising:

a. a lock time after the expiration time;

b. an input for receiving the substitution amount from the substitution transaction;

c. a first refund output comprising a first refund amount and a first condition requiring approval of the second party; and

d. a second refund output comprising a second refund amount and a condition requiring approval of the third party.

Example inchoate substitute refund transaction:

```
Input:

     Previous tx: 9c8b...4794

     Index: 0

     scriptSig: OP_0 [sig. placeholder] b2ac...8a4601

Output:

     Value: 178124000

     scriptPubKey: OP_DUP OP_HASH160 30e6...2511
     OP_EQUALVERIFY OP_CHECKSIG

Output:

     Value: 121866000

     scriptPubKey: OP_DUP OP_HASH160 94e2...4fb6
     OP_EQUALVERIFY OP_CHECKSIG

...

nLockTime: 2014-06-03T12:34:56Z
```

8. The facilitator signs the inchoate substitute refund transaction and transmits the signed substitute refund transaction to the second party and the third party.

9. The facilitator broadcasts the signed substitution transaction.

[67] Various verification and details steps disclosed in previous embodiments have been omitted for brevity. In other embodiments, the transactions are created or signed by the first party or the second party instead of the facilitator. For example, the first party and the second party could agree upon the amounts in the substitution transaction, and each could sign it without involving the facilitator. All such variations are considered part of the invention.

[68] A letter of credit (L/C) is well known in the art, but is fundamentally an agreement where a third party transfers assets to a second party on behalf of a first party upon some agreed upon condition being demonstrated as met before an agreed upon time (an expiration). Typically, this comprises an expensive manual review of arcane shipping documents by an intermediary financial institution before it will release funds on behalf of a buyer. However this costly approach can be eschewed in favor of one embodiment of the invention in which the facilitator conditions the creation and transmission of a disbursement transaction based on the result from a query to a shipper's public API regarding a known tracking number. In other embodiments, L/C terms comprise evaluating search results, observation of the presence or absence of data at an anticipated location, checking that the value of a variable or response from an API is within a set of expected values or matches an anticipated pattern, taking a measurement from an instrument and validating that it is within an anticipated range or tolerance, etc. The possibilities are many and varied. For example, US continuation application 13/970,755 ('755) describes systems and methods for efficiently calculating geospatial nearness. Others are known in the art. In one embodiment, the calculation comprises a condition whereupon an object is or was "at" or "near" (i.e., within a specified distance of) a particular location. Mechanisms to discover the location of said object are known in the art (e.g., self-reporting GPSs, Automatic Identification and Data Capture (AIDC) devices, such as barcodes, Quick Response (QR) Codes, Radio Frequency Identification (RFID) tags, in proximity of a reporting detector or sensor at a known location, etc.). Many possible configurations are contemplated by the invention, and will become apparent to one skilled in the art.

[69] FIG. 8 depicts aspects of one embodiment pertaining to an L/C comprising a source transaction and a commit transaction. As depicted, the commit transaction comprises a first input for accepting a first amount from a first source transaction (i.e., from a first party), and one or more outputs for directing a portion of the first amount to one or more other transactions (not depicted). In other embodiments (portions of which are depicted in other figures), the commit transaction further comprises a second input for accepting a second amount from a second source transaction (i.e., from a second party), where the first amount and second amount

total an expected amount. In some cases the amounts comprise a principal amount (P), and (optionally) a collateral amount (C), as depicted in the various figures. While only a first source transaction is depicted in FIG. 8, that should not be construed as a limitation of the invention.

[70] FIG. 9 depicts aspects of one embodiment pertaining to an L/C comprising a commit transaction and an expiration transaction, the expiration transaction being analogous to the refund transaction in previously described embodiments. However, where a refund transaction is meant exclusively for recovery of funds an exception (e.g., the facilitator becomes unavailable to create or sign a disbursement transaction), use of an expiration transaction, in addition to recovery, is contemplated by the offer (e.g., if the conditions set forth are not satisfied before the expiration time, despite the facilitator being operational). The difference is largely conceptual. The two function almost identically within the invention. The commit transaction comprises a first input for receiving a first principal amount (P_A), and a commit output. The expiration transaction comprises an input for receiving an amount from the commit output, a first expiration output to the first party. In other embodiments where the commit transaction comprises a second input for receiving a second amount, the expiration transaction comprises a second expiration output to the second party.

[71] FIGS. 10-11 depict aspects of L/C embodiments comprising relatively simple disbursement transactions in a situation involving principal and collateral. In FIG. 10, the commit transaction comprises a first joined principal and collateral ($(P+C)_A$) input from a first party. In other embodiments, just as with those mentioned above, the inputs need not be joined. In FIG. 11, the commit transaction comprises a first joined principal and collateral input from a first party, and a second collateral (C_B) input from the second party. These are but two of many possible configurations contemplated by the invention. For example, a commit transaction could comprise a principal input from a first party, a collateral input from a third party (e.g., a guarantor of the first party, not depicted), and a collateral input from a second party.

[72] In the embodiments depicted in FIGS. 10-11, each of the disbursement transactions comprises an input for receiving an amount from the commit output. In FIG. 10, the disbursement transaction comprises a first collateral disbursement output to the first party, a first principal disbursement output to the second party, and an optional fee (φ) output to a third party, where the fee is deducted from the collateral. In FIG. 11, the disbursement transaction comprises a collateral disbursement output to the first party, and a joined principal and collateral disbursement output to the second party. In addition, the commit transaction

comprises an optional fee output to a third party, which is born equally by the parties in the disbursement transaction. Again, these are but two of many possible configurations contemplated by the invention. For example, the optional fee output could be allocated at any stage, or multiple stages. It could be born solely or disproportionately by one party at the same or different stages.

[73] To illustrate by way of example how some of the various components above may be used together to facilitate various L/C agreements, the following steps occur in one embodiment using the Bitcoin or similar protocol as the transfer mechanism, where the parties do not trust each other, and the facilitator is not fully trusted by any of the parties:

10. A first client creates an offer, the offer comprising terms, the terms comprising:

    a. one of a disbursement condition, a reference to a disbursement condition, a disbursement function, and a reference to a disbursement function;

    b. a principal amount;

    c. an expiration time;

    d. optionally, a first collateral amount; and

    e. optionally, a second collateral amount.

    Example terms:

    Payer principal: 0.5 (BTC)

    Payer collateral: 1 × principal

    Payee collateral: 0.05 × principal

    Disbursement condition:

    ```
    FedEx("987654321").deliveredToCarrier() == true
    ```

    Expiration: 2014-06-01T12:34:56Z

    ...

11. The first client signs a first source transaction.

12. The first client creates an inchoate commit transaction comprising:

    a. the first input for receiving the first amount from the first source transaction;

    b. optionally, a second input for receiving a second amount from a second source transaction;

    c. a commit output comprising a commit amount and a condition requiring approval of two of:

        i. a first party;

        ii. a second party; and

        iii. a facilitator.

13. Optionally, the first client transmits the offer to the facilitator, who validates aspects of the offer (e.g., that the facilitator can interpret the terms, that the expiration time is within an acceptable range, etc.). If validation fails, the facilitator may reject the offer, optionally with an error message to the first client.

14. The first client transmits the offer to a second client.

15. Optionally, if the inchoate commit transaction comprises a second input, the first client transmits the inchoate commit offer to the second client. The second client signs a second source transaction. The second client signs the inchoate commit transaction. The second client transmits the inchoate commit transaction back to the first client.

16. The first client signs (e.g., with `SIGHASH_ALL | SIGHASH_ANYONECANPAY`) the inchoate commit transaction to create a complete commit transaction, optionally storing the complete commit transaction in non-transitory memory.

    Example complete commit transaction:

```
ID: c215...fc9b

Input:

    Previous tx: 85f7...e06c

    Index: 4
```

```
        scriptSig: 186b...ed3d81 9a9c...0fc5

    Input:

        Previous tx: 6b03...e16e

        Index: 7

        scriptSig: c48e...353c81 4afe...2c8d

    ...

    Output:

        Value: 150000000

        scriptPubKey: 2 67c1...4a70 bf9a...f9e3 cffd...1373 3
        OP_CHECKMULTISIG

    ...
```

17. The first client signs an inchoate expiration transaction comprising:

    a. a lock time on or after the expiration time;

    b. an input for receiving the commit amount from the complete commit transaction;

    c. a first expiration output comprising a first expiration amount and a first condition requiring approval of the first party; and

    d. optionally, a second expiration output comprising a second expiration amount and a condition requiring approval of the second party.

    Example inchoate expiration transaction:

```
    Input:

        Previous tx: c215...fc9b

        Index: 0

        scriptSig: OP_0 7d17...0b5101 [sig. placeholder]
```

```
...

Output:

      Value: 99995000

      scriptPubKey: OP_DUP OP_HASH160 53a5...8974
      OP_EQUALVERIFY OP_CHECKSIG

Output:

      Value: 4995000

      scriptPubKey: OP_DUP OP_HASH160 30e6...2511
      OP_EQUALVERIFY OP_CHECKSIG

...

nLockTime: 2014-06-01T12:34:56Z
```

18. The first client transmits the complete commit transaction and the inchoate expiration transaction to the second client who optionally stores the complete expiration transaction in non-transitory memory.

19. The second client signs the inchoate expiration transaction to create a complete expiration transaction and stores the complete expiration transaction in non-transitory memory.

20. The second client transmits the complete expiration transaction to the first client.

21. After creating or receiving both the complete commit transaction and the complete expiration transaction, the first client broadcasts the first source transaction.

22. After creating or receiving both the complete commit transaction and the complete expiration transaction, the second client broadcasts the second source transaction.

23. After seeing that both the first source transaction and second source transaction have been broadcast, one or both of the first client the second client broadcast the complete commit transaction.

24. At a time or upon an event as defined by the terms or upon a query by the first client or

the second client (optionally providing one or more of the complete commit transaction, a reference to the complete commit transaction, and the terms), and before the lock time of the complete expiration transaction, the facilitator performs a calculation in accordance with the terms for determining a first disbursement amount, and optionally a second disbursement amount, optionally requesting information from an oracle for use in the calculation (e.g., whether an anticipated shipment has been delivered to a shipper, a destination address, etc., etc.). In one embodiment, the facilitator queries an oracle, which comprises a data source. This could be an external API, internal database, etc.

In a typical embodiment, the disbursement amounts are such that any remaining collateral is returned to the respective providing party, and the principal is transferred from the providing party (payer) to the counterparty (payee).

25. The facilitator signs an inchoate disbursement transaction, which comprises:

a. an input for receiving the commit amount from the complete commit transaction;

b. a first disbursement output comprising the first disbursement amount and a first condition requiring approval of the second party;

c. optionally, a second disbursement output comprising the second disbursement amount and a condition requiring approval of the first party;

d. optionally a third disbursement output comprising a fee amount and a condition requiring approval of a third party;

typically where the sum of the first disbursement amount, any second disbursement amount, and any fee amount is not more than the commit amount from the complete commit transaction.

Example inchoate disbursement transaction:

```
Input:

      Previous tx: c215...fc9b

      Index: 0

      scriptSig: OP_0 [sig. placeholder] 8205...424901
```

Output:

Value: **49990000**

scriptPubKey: **OP_DUP OP_HASH160 30e6...2511 OP_EQUALVERIFY OP_CHECKSIG**

Output:

Value: **54990000**

scriptPubKey: **OP_DUP OP_HASH160 6250...6cfc OP_EQUALVERIFY OP_CHECKSIG**

Output:

Value: **10000**

scriptPubKey: **OP_DUP OP_HASH160 d377...5c8c OP_EQUALVERIFY OP_CHECKSIG**

...

26. The facilitator transmits the inchoate disbursement transaction to both the first client and the second client, either of whom can broadcast it as in the prior example embodiments.

[74] In another embodiment, the condition of the commit output requires approval of either the first party and the second party or the second party and one or more service providers, (e.g., a shipper, insurance provider, inspector, etc.). An inchoate disbursement transaction is constructed with placeholders for the second party, and each of the service providers. When all of the service providers have signed their respective portions, the second party may sign and broadcast the disbursement transaction. In a further embodiment, the second party commits assets to the commit transaction for paying each of the service providers, and each of the service providers are paid out of the disbursement transaction.

[75] FIGS. 12-14 depict transaction chains from various example L/C embodiments comprising substitutions of parties. FIG. 12 depicts aspects of an embodiment where a payer party (A) has convinced a substituting party (C) to substitute into a transaction with a payee

party (B). In addition, the payer party transfers a negotiated amount (ε) to the substituting party. For example, the payer party could have committed to purchasing goods from the payee party, but due to unanticipated market conditions, decided to sell the right to take delivery of the goods to the substituting party at a loss. This is facilitated in the depicted embodiment by a substitution transaction and a second expiration transaction. In a related embodiment where the payer party sold the right to take delivery for a profit, the negotiated amount might flow from the substituting party to the payer party. In the embodiment depicted in FIG. 12, an optional fee (φ) is paid to a third party, and is born by the payee party.

[76] FIG. 13 depicts aspects of an embodiment where a payee party (B) has convinced a substituting party (C) to substitute into a transaction with a payer party (A). In addition, the substituting party transfers a negotiated amount (ε) to the payer party. For example, the third party, may be interested in having the right to receive payment under a future disbursement transaction, perhaps due to the decreasing relative value of the substituting party's other assets. This is facilitated in the depicted embodiment by a substitution transaction, and a second expiration transaction. In a related embodiment where the payee party sold the right to receive payment at a loss, the negotiated amount might flow from the payee party to the substituting party. Similar to FIG. 12, in the embodiment depicted in FIG. 13, an optional fee (φ) is paid to a third party, and is born by the substituting party.

[77] FIG. 14 depicts aspects of an embodiment where a payer party (A) has convinced a substituting party (C) to substitute in part (as depicted to cover the collateral originally paid by the payer party) into a transaction with a payee party (B). In addition, the substituting party transfers a negotiated amount (ε) to the payer party. This is facilitated in the depicted embodiment by a substitution transaction and a second expiration transaction. In some embodiments, the substitution output of the substitute transaction comprises a condition requiring approval of three of three parties, three of four parties, or two of four parties (e.g., where the substituting party has been delegated authority to approve or sign on behalf of itself and for the payer party). Many possible configurations are contemplated by the invention. In such embodiments, the facilitator can act as a referee in creating the substitution transaction to the satisfaction of all parties, for example, maintaining the ability to dispute the transaction with a chosen mediator as described below.

[78] For clarity of illustration in FIGS. 12-14, the outputs of the commit transaction and the corresponding inputs of the substitution transaction are depicted as separate for each of the first

joined principal and collateral ($(P+C)_A$), and the second collateral (C_B). This is not a limitation of the invention. The outputs of the commit transaction, and corresponding inputs of the substitution transaction could be any configuration considered valid by the transfer mechanism. The outputs of the substitution transaction and inputs to the second commit transaction are similarly depicted for clarity of illustration. Again, all valid configurations of inputs and outputs between transactions are contemplated by the invention. Also, in other embodiments, any fee could be paid, in part or in whole, by any party, even a fourth party.

[79] Where the Bitcoin protocol, the Ethereum protocol, or similar is used as the transfer mechanism, another embodiment of the invention enables arbitrary offers—such as offers for arbitrary swaps, L/Cs, and any other offer where terms describing that may be expressed and interpreted by the facilitator—to be made by broadcasting a specialized transaction in which the terms, a reference to the terms (e.g., a URI for the terms, a hash of the terms, etc.), or some combination thereof is encoded into the offer transaction itself, rather than associated via an extra transfer mechanism means (i.e., "off blockchain" in Bitcoin protocol terms), such as a centralized authority, or shared decentralized data store (e.g., a torrent, an "altcoin", etc.).

[80] In one embodiment, this could be encoded as transaction metadata, or—where the Bitcoin Protocol or similar is used as the transfer mechanism—unused data in an input or output (e.g., `<data> OP_DROP <script>`, via the `OP_RETURN <data>` technique in a single output, etc.). For illustration, the following steps describe but a few of many such embodiments:

1. In one embodiment, a first client (offeror) creates an offer transaction comprising associated data and an offer output comprising an offer amount and a condition requiring approval of one of a first party and, optionally, a facilitator. The associated data comprise one or both of terms and a reference to the terms. Optionally, the associated data comprise a reference to the facilitator (e.g., a domain name, a payment address, D&B number, URI, etc.). Also optionally, the first client transmits the terms, the associated data, or offer transaction to the facilitator for validation before broadcasting it (e.g., to ensure the facilitator can interpret the terms, that the facilitator is appropriately identified, etc.). In another embodiment, at the first client's request, the facilitator creates an inchoate offer transaction (e.g., not including a signed input) for creating a complete offer transaction, and the first client optionally verifies whether the facilitator created the transaction correctly, whether it's available via the facilitator-provided reference (if applicable), etc.

Example inchoate offer transaction:

```
% # Post the terms to the facilitator
% curl -X POST -d
'{"base":"USD","quote":"AUD","denom":"BTC","pcpl":0.5,"cltl":1.0,
"res":"symunbound","offerexp":"2014-06-
01T00:00:00Z","swapexp":"2014-07-
01T00:00:00Z","facuri":"https://facilitator.dom/api/v1"}' ...
https://facilitator.dom/api/v1/swap
{"ok":true,"offersha256":"3a72...f9a4","offerref":"facswap:3a72..
.f9a4","offeruri":"https://facilitator.dom/api/v1/swap/3a72...f9a
4"}

     ID: 9fcd...429c

     ...

     Output:

          Value: 150000000

          scriptPubKey: 666163737761703a3a72...f9a4 OP_DROP 1
          67c1...4a70 cffd...1373 2 OP_CHECKMULTISIG

     ...
```

"666163737761703a" is hexidecimal for the eight byte ascii string "facswap:".

Alternate embodiment example offer transaction:

```
% # Post the terms to the facilitator
% curl -X POST -d '{"pubkey":"67c1...4a70","terms":
{"base":"USD",...,"facuri":"https://facilitator.dom/api/v1"}}' ..
. https://facilitator.dom/api/v1/swap
{"ok":true,"offersha256":"3a72...f9a4","offerref":"facswap:3a72..
.f9a4","offeruri":"https://facilitator.dom/api/v1/swap/3a72...f9a
4","offertxn":"04000000...0280d1f008000000008901014b67c1...4a704b
cffd...13730102ae...00000000000000002a6a28666163737761703a3a72...
f9a400000000"}
```

```
% # Validate "offertxn", add change outputs, etc.
```

"offertxn" is annotated as follows:

```
04000000 [version: 4] ... 02 [output count: 1] 80d1f00800000000
[amount: 1.5 BTC] 89 [script len: 137] 01 [push next 1 byte] 01
[1] 4b [push next 75 bytes] 67c1...4a70 [pub. key] 4b [push next
75 bytes] cffd...1373 [fac. pub. key] 01 [push next 1 byte] 02
[2] ae [OP_CHECKMULTISIG] ... 0000000000000000 [amount: 0.0 BTC]
2a [script len: 42] 6a [OP_RETURN] 28 [push next 40 bytes]
666163737761703a3a72...f9a4 [offerref: "facswap:3a72...f9a4"]
00000000 [lock time: none]
```

Note that some parts (such as any inputs or input placeholders) have been skipped with ellipses to assist with readability. In an alternate embodiment, Pay-to-Script Hash (P2SH) is used.

2. In one embodiment, the first client creates, or, in another embodiment, the facilitator creates an inchoate commit transaction for creating a complete commit transaction much like those described in previous embodiments, except whose first commit input is for accepting the offer amount from the offer transaction, and whose second input is for accepting an amount from a source transaction yet to be identified.

3. The first client signs and broadcasts the signed offer transaction.

4. The facilitator receives the broadcast signed offer transaction.

5. A second client transmits a public key to the facilitator.

6. The facilitator adds the public key to the inchoate commit transaction and transmits the inchoate commit transaction to the second client.

7. The second client signs a source transaction having a transaction ID.

8. The second client adds the transaction ID to the inchoate commit transaction and signs it.

Example inchoate commit transaction:

```
Input:

      Previous tx: 9fcd...429c

      Index: 0

      scriptSig: [sig. placeholder]

Input:

      Previous tx: b5e8...6f57

      Index: 6

      scriptSig: 9b6b...8f3701 ac2f...b01b

...

Output:

      Value: 149990000

      scriptPubKey: 2 67c1...4a70 dbe4...4cbe cffd...1373 3
      OP_CHECKMULTISIG

...
```

9. The second client transmits the signed inchoate commit transaction to the facilitator.

10. Either the first client or, optionally (where allowed), the facilitator creates the complete commit transaction (e.g., `ID: 6996...ec3d`) by signing the inchoate commit transaction, optionally storing the complete commit transaction in non-transitory memory.

    Embodiments where one of the first party and the facilitator can approve spending the offer output require the first party to trust the facilitator to perform some verification (e.g., that the second source transaction has sufficient assets, that a nefarious party is not attempting to commit a huge number of very tiny inputs such that the mining fee will be large, or difficult to meet, etc.) and to craft the commit transaction correctly and consistently with the terms.

11. The facilitator creates an inchoate refund or expiration transaction and transmits the inchoate refund or expiration transaction to the second client.

12. The second client signs the inchoate refund or expiration transaction and transmits the signed inchoate refund or expiration transaction to the facilitator.

13. Either the first client or, optionally (where allowed), the facilitator creates the complete refund or expiration transaction by signing the inchoate refund transaction, storing the complete refund or expiration transaction in non-transitory memory.

14. The facilitator transmits the complete commit transaction and the complete refund or expiration transaction to the second client.

15. The second client broadcasts the source transaction.

16. After seeing that the source transaction has been broadcast, one, several, or all of the first client, the second client, and the facilitator broadcast the complete commit transaction, after which the process is analogous to previously described embodiments.

[81] In an alternate embodiment, the offer comprises a "hard offer", the condition of the offer output requires approval of both the first party and the facilitator, and the facilitator signs and transmits to the first party an offer expiration transaction comprising a lock time set to the time the hard offer expires, an input for receiving the offer amount, and an expiration output comprising an expiration amount and a condition requiring approval of the first party.

[82] In other embodiments of the invention, the transacting parties agree on a third party to act as a mediator in a dispute. For example, if the facilitator becomes unavailable, rather than electing to invoke a refund, one party triggers a dispute whereby a mediator stands in place of the unavailable facilitator. The condition of the commit output of the complete commit transaction requires approval of two of the first party, the second party, the facilitator, and the mediator. On or after the expiration time, or at a time or upon an event as defined by the terms, and before the lock time of the complete refund transaction, each of the disputing party and the mediator signs and one party broadcasts a dispute transaction comprising an input for receiving the commit amount from the complete commit transaction, and a dispute output comprising a dispute amount and a condition requiring approval of two of the first party, the second party, and the mediator. Once the dispute as been resolved, either the parties sign, or the mediator and one of the parties sign a settlement transaction similar to the disbursement transaction above,

but reflecting the mediated settlement.

[83] FIGS. 15-16 depict aspects of two such embodiments. In FIG. 15, the dispute transaction further comprises a first fee output comprising a facilitator fee amount (φ_X) and second fee output comprising a mediator fee amount (φ_M), the fees being shared by the parties. In FIG. 16, the dispute transaction comprises the facilitator fee amount shared by the parties, and the settlement transaction comprises the mediator fee amount paid by the party that initiated the dispute (B). In another embodiment, any mediator fee is determined as a term of the settlement, and included with the settlement transaction.

[84] Optionally (and preferably), the parties also sign and transmit to each other a dispute refund transaction similar to that above, but instead taking its input from the dispute transaction, and with a lock time set in the future with enough time to reach a settlement. This way if the mediator becomes unavailable, the parties can again revert to broadcasting a refund. In another embodiment, the dispute transaction could also be "mediatable", allowing for a chain of such disputes, for example naming a second mediator in the event that the mediator becomes unavailable, or the same mediator to allow more time to reach a settlement if the lock time of the dispute refund transaction is approaching.

[85] In other embodiments, mediation can be automated. For example, in embodiments pertaining to swaps or similar transactions, the facilitator periodically transmits an unsigned disbursement transaction to the parties as if the trade were halted at the time the unsigned disbursement transaction is created. The unsigned disbursement transaction comprises a verifiable time at which it was created, or a reference to such a time (e.g., where the transfer mechanism is the Bitcoin or similar protocol, as unused but signed data embedded in one of the scripts, signature by a separate key owned by the facilitator, but not used for signing any inputs, etc.). If the facilitator becomes unavailable before it can transmit the signed disbursement transaction, and remains unavailable past the expiration time, a dispute could be initiated, and the parties would have a window during which they have an opportunity to transmit the terms (preferably signed by each party, but this is not necessary if the parties agree on the terms, i.e., both transmit the same terms to the mediator) and some or all of the unsigned disbursement transactions they received from the facilitator to the mediator. The mediator examines the terms and the disbursement transactions presented by both parties. The mediator examines the undisputed or signed terms, and all verifiable unsigned disbursement transactions received from both parties. In one embodiment, the mediator merely selects the most recent verifiable

unsigned disbursement transaction. In another embodiment, the mediator "plays back" the unsigned disbursement transactions in order, verifying whether any unsigned disbursement transaction should have triggered an early exit to the trade (e.g., if collateral was exhausted). In yet another embodiment, the mediator performs its own independent evaluation of the terms, possibly requesting information from an oracle, to stand in place of the facilitator by creating a new settlement transaction as close to the disbursement transaction that would have been created by the facilitator if it was available as the mediator is able to determine.

[86] Note that the depicted embodiments are among the more basic of the invention. The various combinations of source transactions, commit transactions, disbursement transactions, refund transactions, expiration transactions, inputs, outputs, and parties, as well as any principal, collateral, or fees, are limited only by the agreements among the participating parties and are enabled by the invention. Additionally, certain steps of the embodiments disclosed throughout this application are described as being performed by certain entities. In other embodiments, similar or equivalent steps could be performed—wholly or partly—by different parties in lieu of or in addition to those described herein. All such embodiments are considered within the scope of the invention.

[87] As a very simple example, in an embodiment using the Bitcoin protocol, the Ethereum protocol, or similar, transactions use P2SH in place of multi-sig transactions. Other steps may be omitted in certain embodiments. For example, in an embodiment using the Bitcoin or similar protocol, the creation of the signed complete refund or expiration transaction—while highly recommended as a contingency to avoid loss in case the facilitator or counterparty disappears or becomes uncooperative—is not strictly necessary to practice the invention. In embodiments involving a mediator, an unsigned dispute transaction could be created by the facilitator and transmitted to the parties for use with the mediator, for example, at the time the refund or expiration transaction is created and transmitted.

INDUSTRIAL APPLICABILITY

[88] The invention pertains to agreements among distinct parties that contemplate transfer of title to property, as well as any industry where that may be of value or importance.

CLAIMS

What is claimed is:

1. A method for performing low-trust or zero-trust transactions between a first client at least intermittently connected to a second client, the method comprising the steps:

    a. creating an offer, the offer comprising:

        i. terms comprising:

            A. a principal amount; and

            B. an expiration time;

    b. creating a commit transaction in accordance with the terms, the commit transaction comprising:

        i. a first principal input for receiving a first principal amount;

        ii. a second principal input for receiving a second principal amount; and

        iii. a commit output comprising a commit amount;

    c. creating a digital signature to associate with the commit transaction by the first client using a first asymmetric key pair;

    d. creating a digital signature to associate with the commit transaction by the second client using a second asymmetric key pair;

    e. broadcasting the signed commit transaction onto a computer network accessible by a transfer mechanism.

2. The method of claim 1, where the terms further comprise a collateral amount, where the commit transaction further comprises one or both of an input for receiving a first collateral amount and an input for receiving a second collateral amount.

3. The method of claim 1, where the commit transaction further comprises a fee output comprising a fee amount and a fee condition requiring approval from a third party.

4. The method of claim 1, where the terms further comprise:

a. a reference to a base asset; and

b. a reference to a quote asset.

5. The method of claim 4 further comprising the steps:

a. creating a refund transaction comprising:

i. a lock time after the expiration time;

ii. an input for receiving the commit amount from the commit transaction;

iii. a first refund output comprising a first refund amount and a first refund condition requiring approval from a first party; and

iv. a second refund output comprising a second refund amount and a second refund condition requiring approval from a second party; and

b. storing the refund transaction in a non-transitory computer memory.

6. The method of claim 5 further comprising the steps:

a. calculating a first disbursement amount and a second disbursement amount in accordance with the terms;

b. creating a disbursement transaction comprising:

i. an input for receiving the commit amount from the commit transaction;

ii. a first disbursement output comprising a first disbursement amount and a first disbursement condition requiring approval from the first party; and

iii. a second disbursement output comprising a second disbursement amount and a second disbursement condition requiring approval from the second party; and

c. broadcasting the disbursement transaction onto the computer network before the lock time of the refund transaction.

7. The method of claim 4 further comprising the steps:

a. calculating a first disbursement amount and a second disbursement amount in accordance with the terms;

b. creating a disbursement transaction comprising:

i. an input for receiving the commit amount from the commit transaction;

ii. a first disbursement output comprising the first disbursement amount and a first disbursement condition requiring approval from the first party; and

iii. a second disbursement output comprising the second disbursement amount and a second disbursement condition requiring approval from the second party; and

c. broadcasting the disbursement transaction onto the computer network.

8. The method of claim 7, where the step of calculating the first disbursement amount and the second disbursement amount in accordance with the terms is performed on or after the expiration time.

9. The method of claim 7, where the disbursement transaction further comprises a fee output comprising a fee amount and a fee condition requiring approval from a third party.

10. The method of claim 1, where the terms further comprise:

a. a disbursement condition.

11. The method of claim 10 further comprising the steps:

a. creating an expiration transaction comprising:

i. a lock time after the expiration time;

ii. an input for receiving the commit amount from the commit transaction; and

iii. an expiration output comprising an expiration amount and an expiration condition requiring approval from a first party; and

b. storing the expiration transaction in a non-transitory computer memory.

12. The method of claim 10 further comprising the steps:

a. calculating a disbursement amount in accordance with the terms;

b. creating a disbursement transaction comprising:

i. an input for receiving the commit amount from the commit transaction;

ii. a disbursement output comprising the disbursement amount and a disbursement condition requiring approval from the second party; and

c. broadcasting the disbursement transaction onto the computer network.

13. The method of claim 12, where the step of calculating the disbursement amount in accordance with the terms is performed on or after the expiration time.

14. The method of claim 12, where the disbursement transaction further comprises a fee output comprising a fee amount and a fee condition requiring approval from a third party.

15. The method of claim 11 further comprising the steps:

a. creating a dispute transaction comprising:

i. an input for receiving the commit amount from the commit transaction; and

ii. a dispute output comprising a dispute amount; and

b. broadcasting the dispute transaction onto the computer network before the lock time of the expiration transaction.

16. The method of claim 15, where the dispute transaction further comprises a fee output comprising a fee amount and a fee condition requiring approval from a third party.

17. The method of claim 15 further comprising the steps:

a. creating a settlement transaction comprising:

i. an input for receiving the dispute amount from the dispute transaction;

ii. one of:

A. a first settlement output comprising a first settlement amount and a first settlement condition requiring approval from a first party; and

B. a second settlement output comprising a second settlement amount and a second settlement condition requiring approval from a second party; and

b. broadcasting the settlement transaction onto the computer network.

18. The method of claim 17, where the dispute transaction further comprises a fee output comprising a fee amount and a fee condition requiring approval from a third party.

19. The method of claim 5 further comprising the steps:

a. creating a substitution transaction comprising:

i. a commit input for receiving the commit amount from the commit transaction;

ii. an entry input for receiving an entry amount;

iii. a withdrawal output comprising a withdrawal amount and a first condition requiring approval of one of the first party and the second party; and

iv. a substitution output comprising a substitution amount;

b. creating a digital signature to associate with the substitution transaction by a third client using a third asymmetric key pair; and

c. broadcasting the substitution transaction onto the computer network before the lock time of the refund transaction.

20. The method of claim 19, where the substitution transaction further comprises a fee output comprising a fee amount and a fee condition requiring approval from a third

party.

21. The method of claim 19 further comprising the steps:

    a. creating a substitute refund transaction comprising:

        i. a lock time after the expiration time;

        ii. an input for receiving the substitution amount from the substitution transaction;

        iii. a first refund output comprising a first refund amount and a first refund condition requiring approval from a third party; and

        iv. a second refund output comprising a second refund amount and a second refund condition requiring approval from a second party; and

    b. storing the substitute refund transaction in a non-transitory computer memory.

22. The method of claim 21 further comprising the steps:

    a. calculating a first disbursement amount and a second disbursement amount in accordance with the terms;

    b. creating a disbursement transaction comprising:

        i. an input for receiving the substitution amount from the substitution transaction;

        ii. a first disbursement output comprising a first disbursement amount and a first disbursement condition requiring approval from the third party; and

        iii. a second disbursement output comprising a second disbursement amount and a second disbursement condition requiring approval from the second party; and

    c. broadcasting the disbursement transaction onto the computer network before the lock time of the substitute refund transaction.

23. The method of claim 22, where the step of calculating the first disbursement amount and the second disbursement amount in accordance with the terms is performed on or after

the expiration time.

24. The method of claim 22, where the disbursement transaction further comprises a fee output comprising a fee amount and a fee condition requiring approval from a third party.

25. A system for performing low-trust or zero-trust swap transactions comprising terms, the system comprising a facilitator coupled to a computer network accessible by a transfer mechanism, the facilitator comprising:

a. an interface for receiving terms comprising:

i. a reference to a base asset;

ii. a reference to a quote asset;

iii. a principal amount; and

iv. an expiration time;

b. a first non-transitory memory for storing a first asymmetric key pair; and

c. a first computer processor configured for one of:

i. transmitting a transaction to a client, the client comprising:

A. an interface for receiving a transaction;

B. a second non-transitory memory for storing a second asymmetric key pair and a transaction; and

C. a second computer processor configured for one of:

I. signing a transaction using the second asymmetric key pair; and

II. transmitting a signed transaction over the computer network;

ii. signing a transaction using the first asymmetric key pair;

iii. calculating a first disbursement amount and a second disbursement amount in accordance with the terms;

iv. creating a disbursement transaction comprising:

A. a first disbursement output comprising a first disbursement amount and a first disbursement condition requiring approval from a first party; and

B. a second disbursement output comprising a second disbursement amount and a second disbursement condition requiring approval from a second party; and

v. broadcasting the disbursement transaction onto the computer network.

26. The system of claim 25, where the second non-transitory memory is further for storing a complete transaction.

27. The system of claim 25, where the first computer processor is the second computer processor, and where the first non-transitory memory is the second non-transitory memory.

ABSTRACT

Systems and methods enabling parties with little trust or no trust in each other to enter into and enforce agreements conditioned on input from or participation of a third party, over arbitrary distances, without special technical knowledge of the underlying transfer mechanism(s), optionally affording participation of third-party mediators, substitution of transferors and transferees, term substitution, revision, or reformation, etc. Such transactions can occur reliably without involving costly third-party intermediaries who traditionally may otherwise be required for such transactions, and without traditional exposure to counterparty risk..

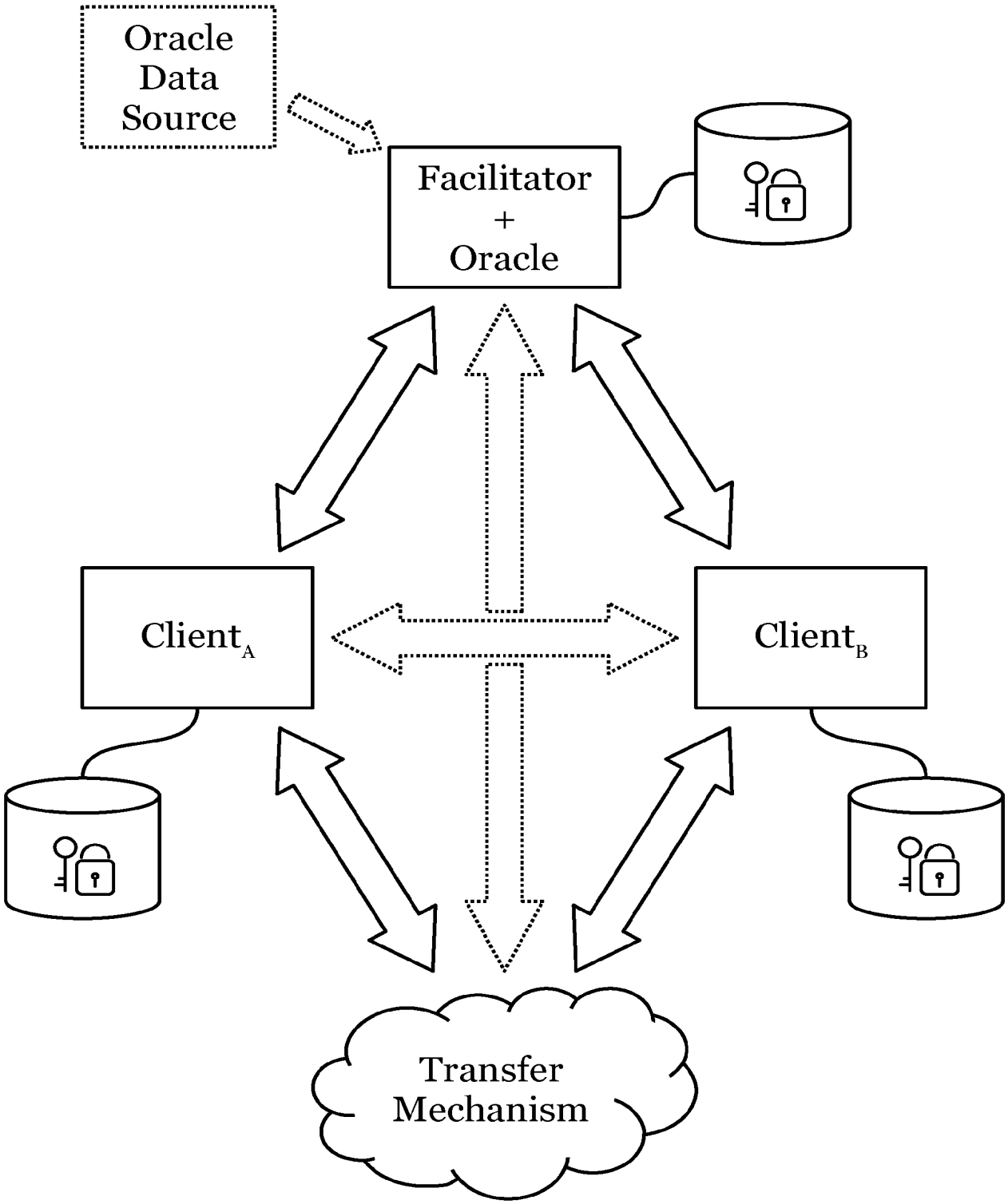

Oracle Data Source
Facilitator + Oracle
Client$_A$
Client$_B$
Transfer Mechanism

FIG. 1

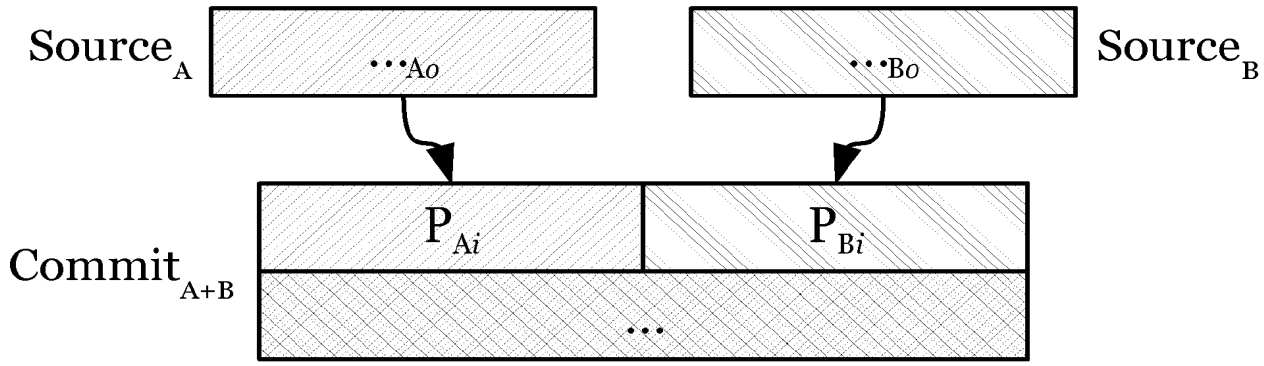

Source A
···Ao
···Bo
Source B
Commit A+B
P Ai
P Bi
...

FIG. 2

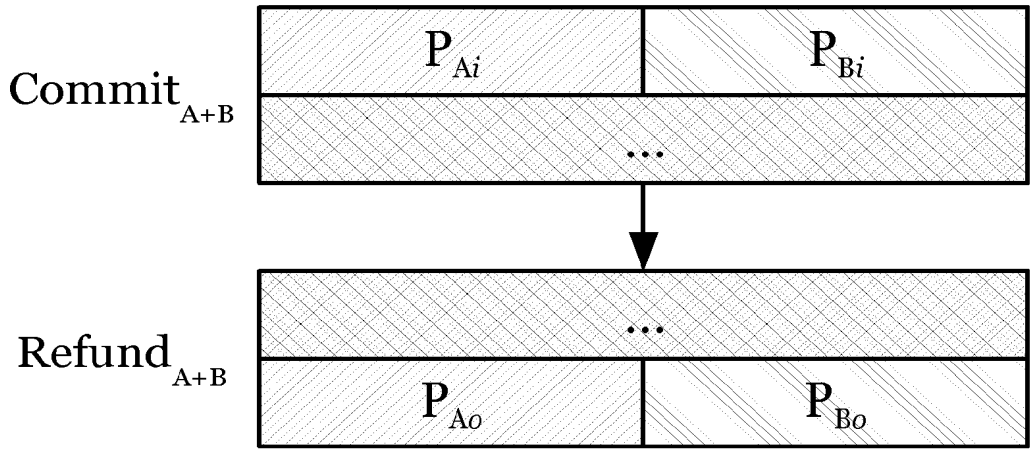

Commit A+B
P Ai
P Bi
...
Refund A+B
...
P Ao
P Bo

FIG. 3

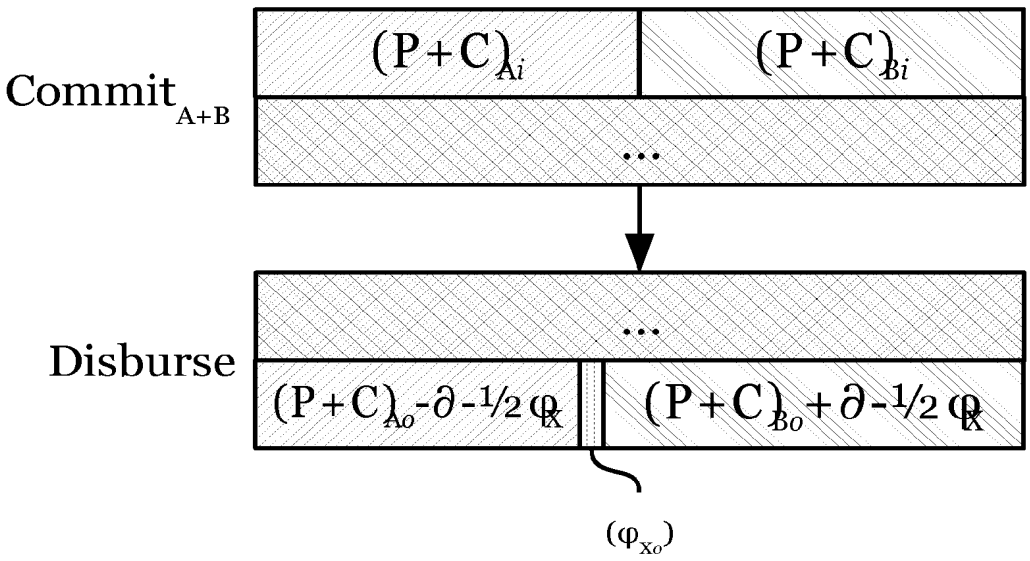

Commit A+B
(P+C)Ai
(P+C)Bi
...
Disburse
...
(P+C)Ao-∂-½φX
(P+C)Bo+∂-½φX
(φXo)

FIG. 4

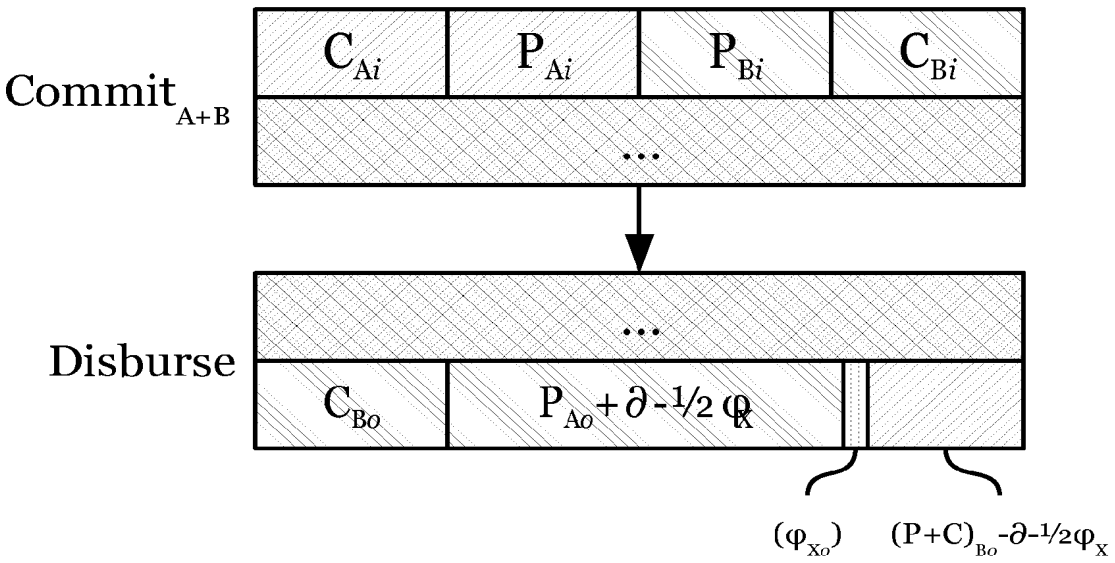

Commit A+B
CAi
PAi
PBi
CBi
...
Disburse
...
CBo
PAo+∂-½φX
(φXo)
(P+C)Bo-∂-½φX

FIG. 5

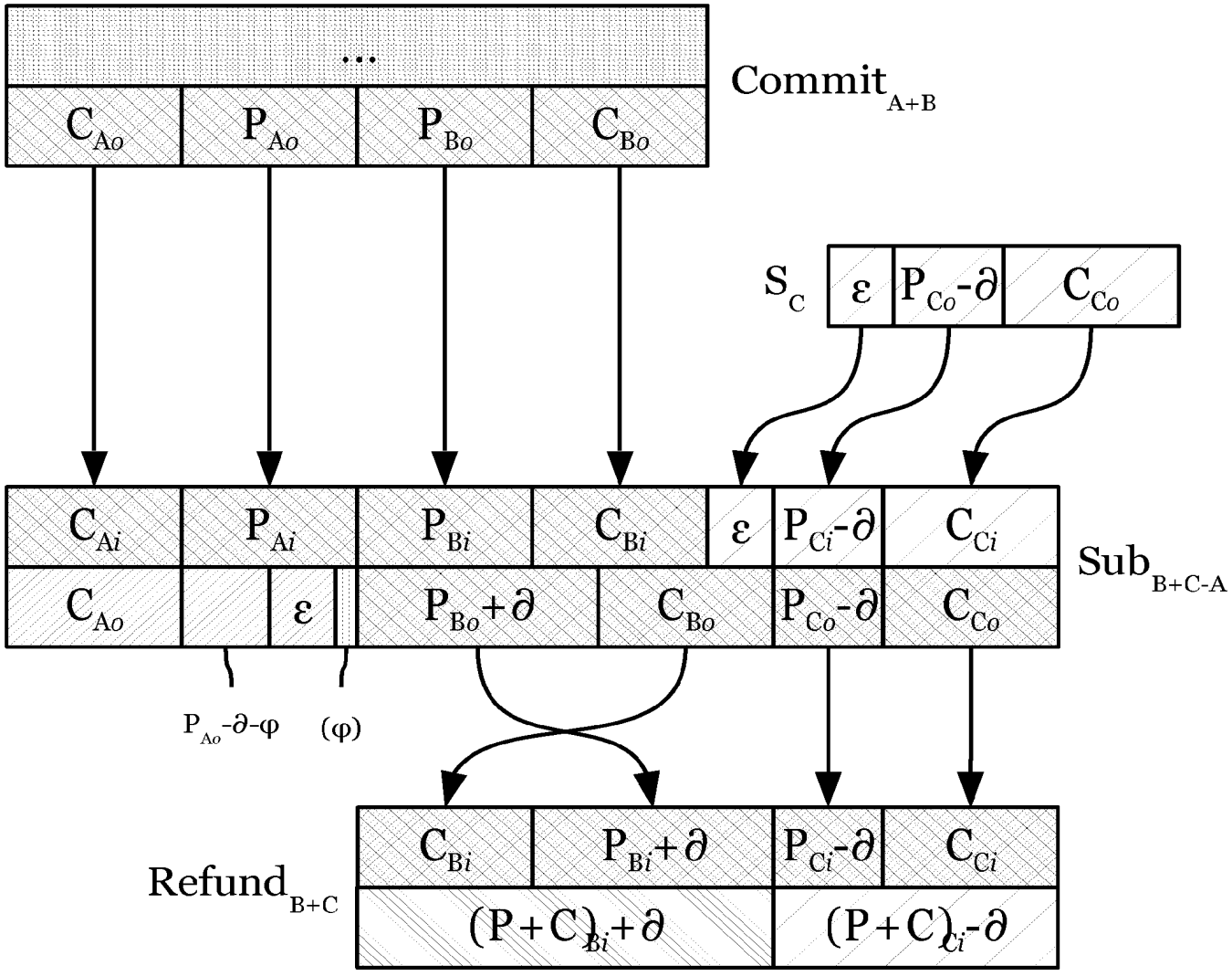

...
C_{Ao}
P_{Ao}
P_{Bo}
C_{Bo}
$Commit_{A+B}$
S_C
ε
P_{Co}-∂
C_{Co}
C_{Ai}
P_{Ai}
P_{Bi}
C_{Bi}
ε
P_{Ci}-∂
C_{Ci}
Sub_{B+C-A}
C_{Ao}
ε
P_{Bo}+∂
C_{Bo}
P_{Co}-∂
C_{Co}
P_{Ao}-∂-φ
(φ)
$Refund_{B+C}$
C_{Bi}
P_{Bi}+∂
P_{Ci}-∂
C_{Ci}
$(P+C)_{Bi}$+∂
$(P+C)_{Ci}$-∂

FIG. 6

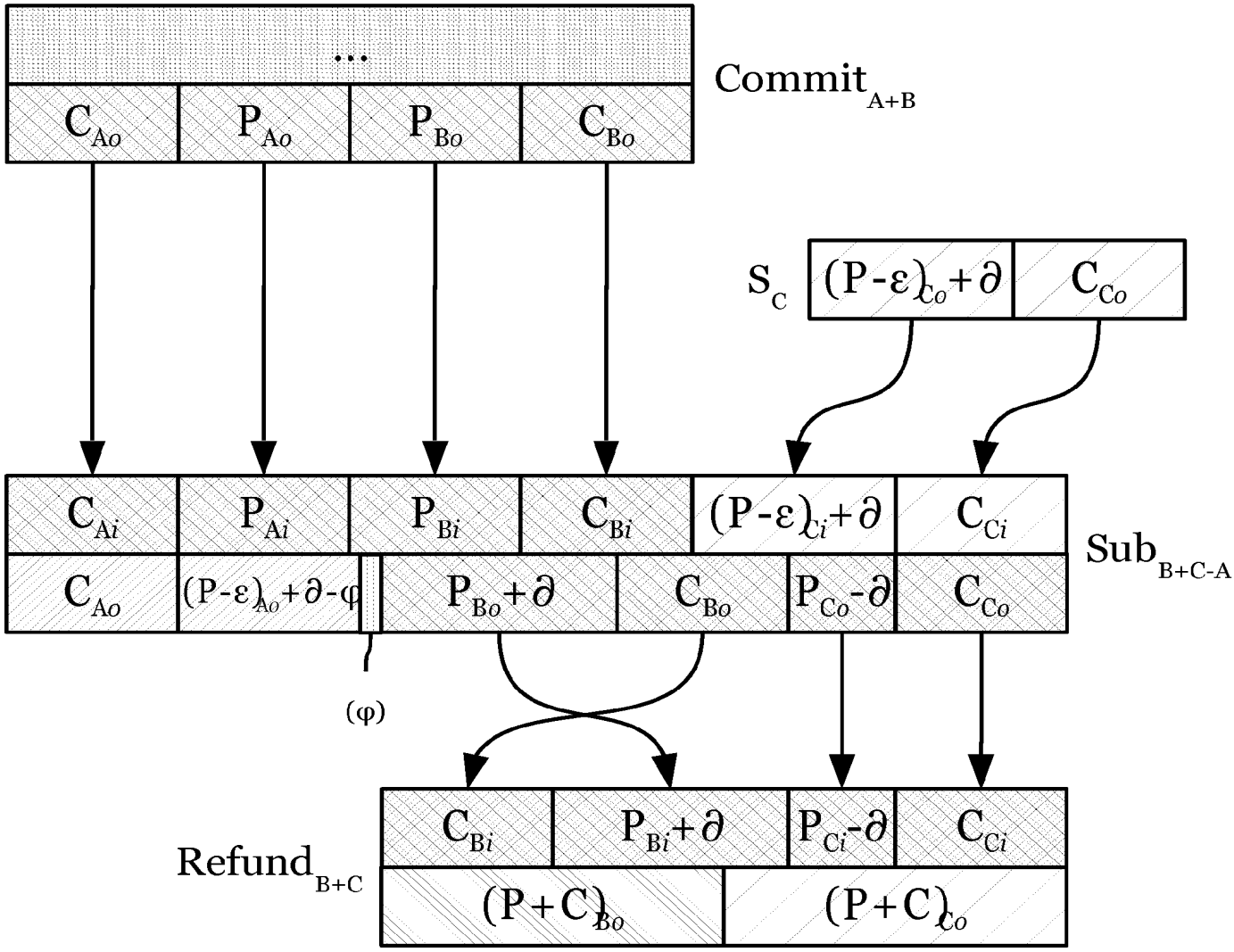

...
C_{Ao}
P_{Ao}
P_{Bo}
C_{Bo}
$Commit_{A+B}$
S_C
$(P-\varepsilon)_{Co}+\partial$
C_{Co}
C_{Ai}
P_{Ai}
P_{Bi}
C_{Bi}
$(P-\varepsilon)_{Ci}+\partial$
C_{Ci}
Sub_{B+C-A}
C_{Ao}
$(P-\varepsilon)_{Ao}+\partial-\varphi$
$P_{Bo}+\partial$
C_{Bo}
$P_{Co}-\partial$
C_{Co}
(φ)
$Refund_{B+C}$
C_{Bi}
$P_{Bi}+\partial$
$P_{Ci}-\partial$
C_{Ci}
$(P+C)_{Bo}$
$(P+C)_{Co}$

FIG. 7

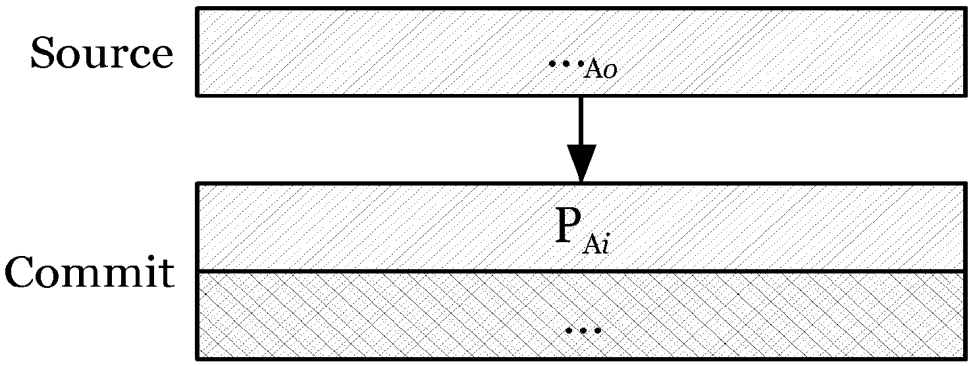


FIG. 8

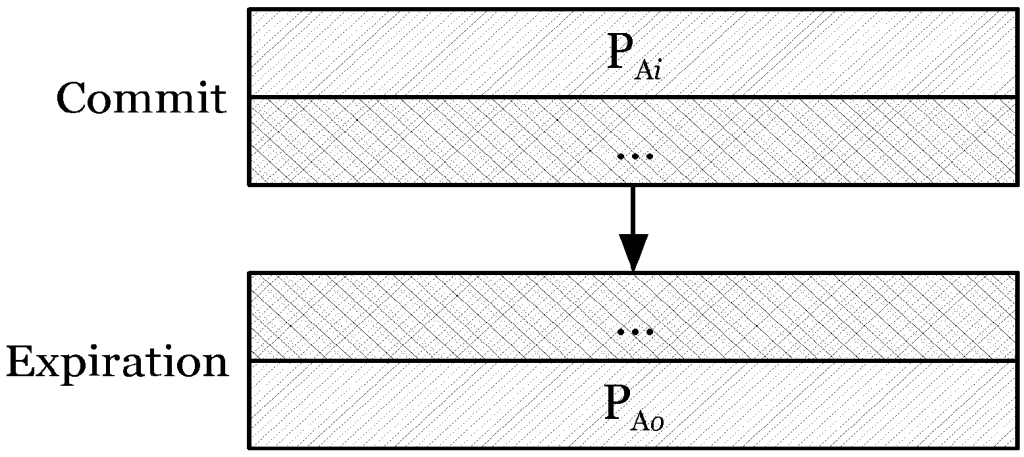


FIG. 9

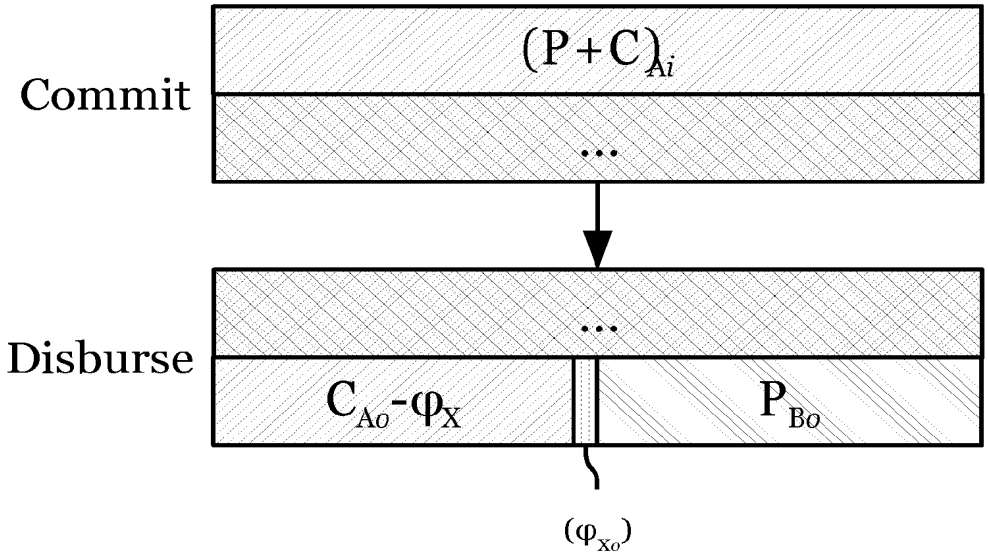

Commit
$(P+C)_{Ai}$
...
Disburse
...
C_{Ao}-φ_X
P_{Bo}
(φ_{Xo})

FIG. 10

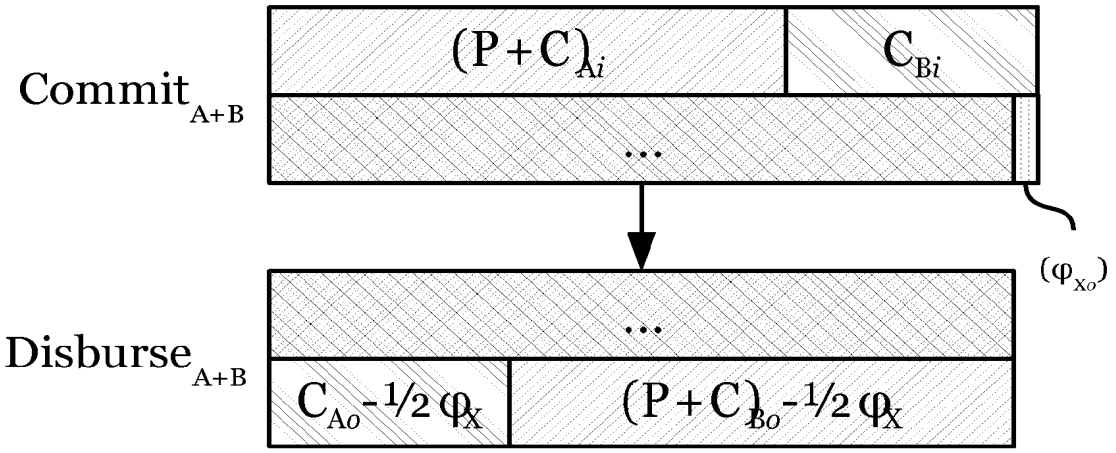

Commit$_{A+B}$
$(P+C)_{Ai}$
C_{Bi}
...
(φ_{Xo})
Disburse$_{A+B}$
...
C_{Ao}-½ φ_X
$(P+C)_{Bo}$-½ φ_X

FIG. 11

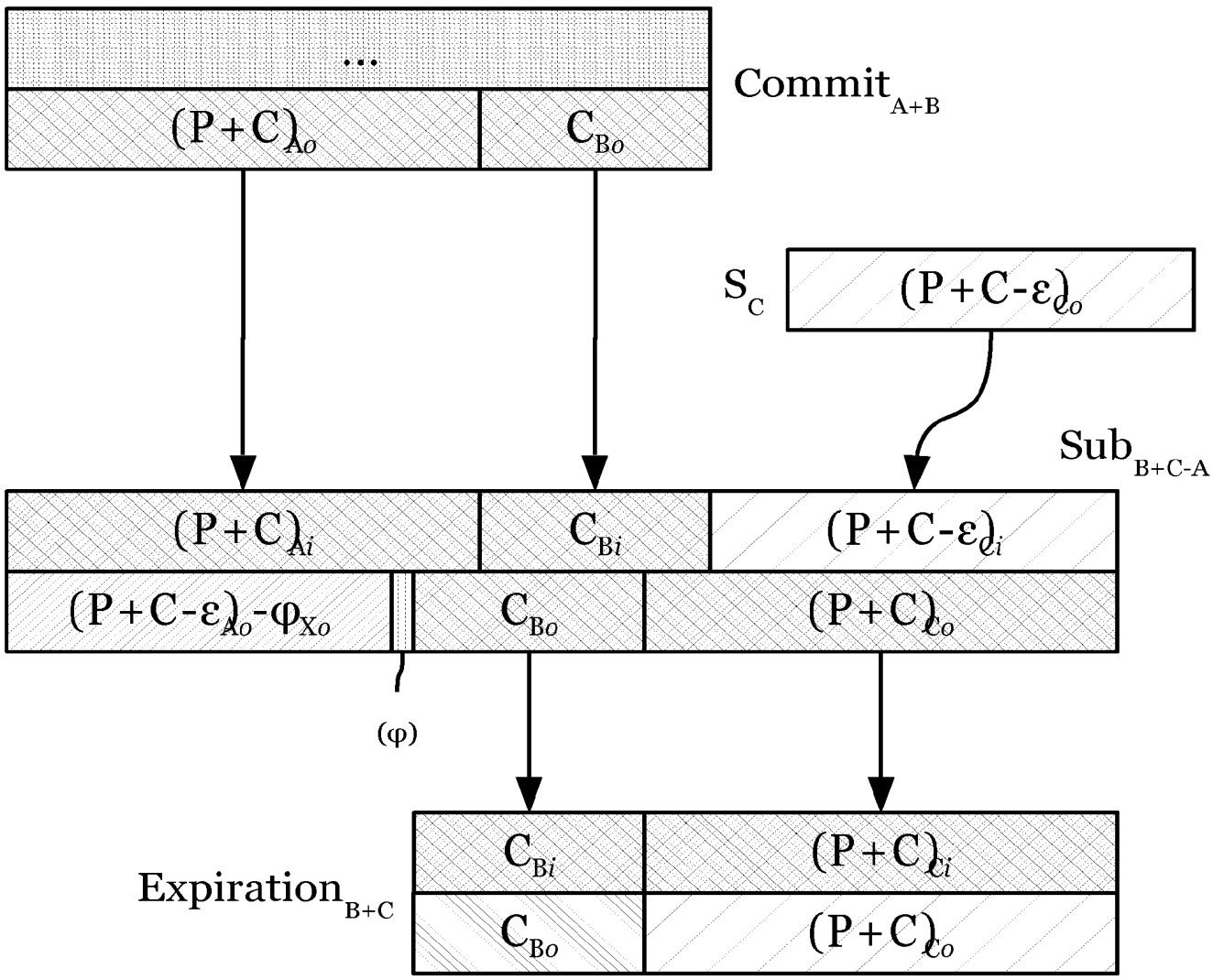

...
$(P+C)_{Ao}$
C_{Bo}
$Commit_{A+B}$
S_C
$(P+C-\varepsilon)_{Co}$
Sub_{B+C-A}
$(P+C)_{Ai}$
C_{Bi}
$(P+C-\varepsilon)_{Ci}$
$(P+C-\varepsilon)_{Ao}-\varphi_{Xo}$
C_{Bo}
$(P+C)_{Co}$
(φ)
$Expiration_{B+C}$
C_{Bi}
$(P+C)_{Ci}$
C_{Bo}
$(P+C)_{Co}$

FIG. 12

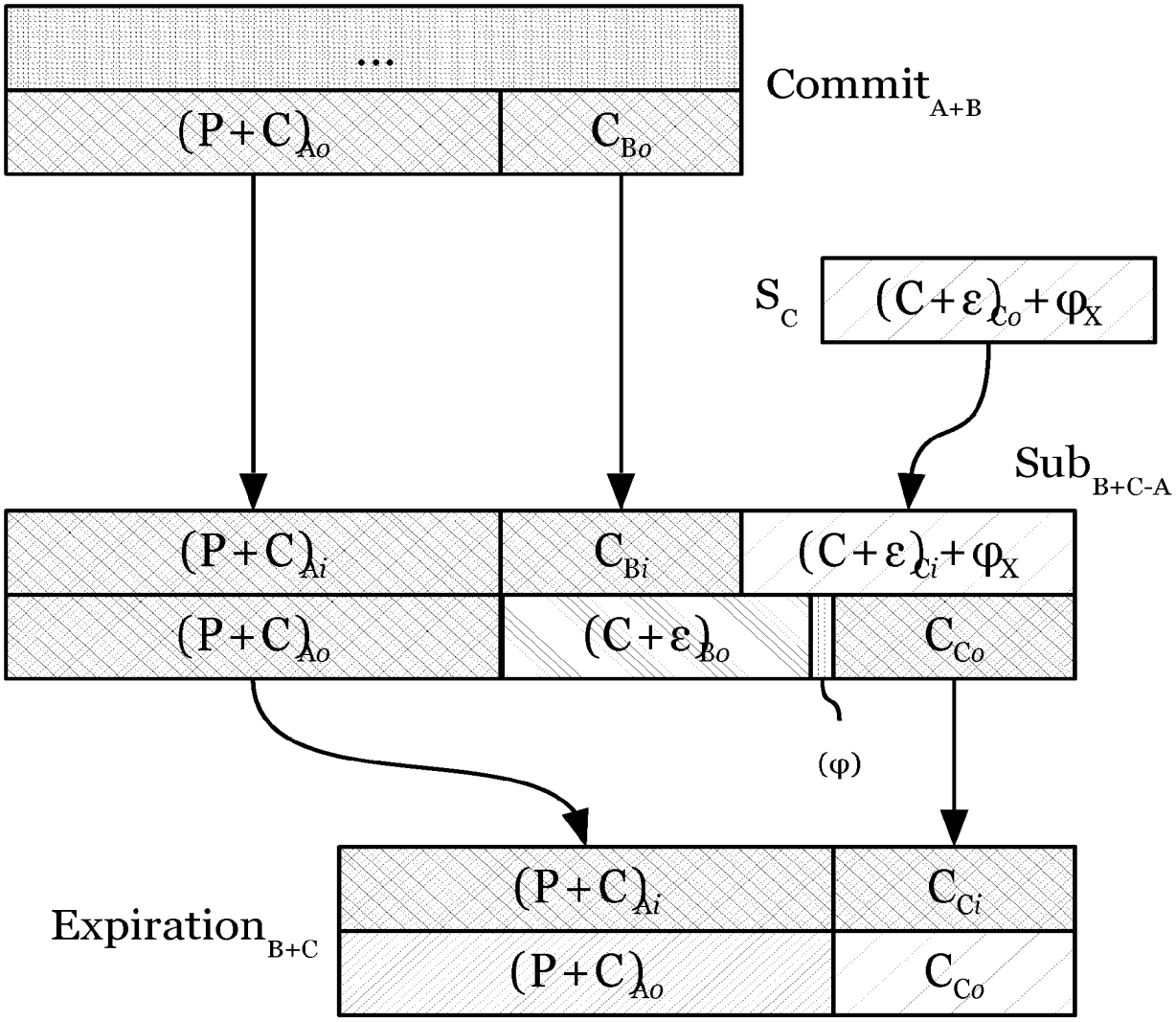

...
Commit A+B
(P+C)Ao
CBo
SC
(C+ε)Co+φX
Sub B+C-A
(P+C)Ai
CBi
(C+ε)Ci+φX
(P+C)Ao
(C+ε)Bo
CCo
(φ)
Expiration B+C
(P+C)Ai
CCi
(P+C)Ao
CCo

FIG. 13

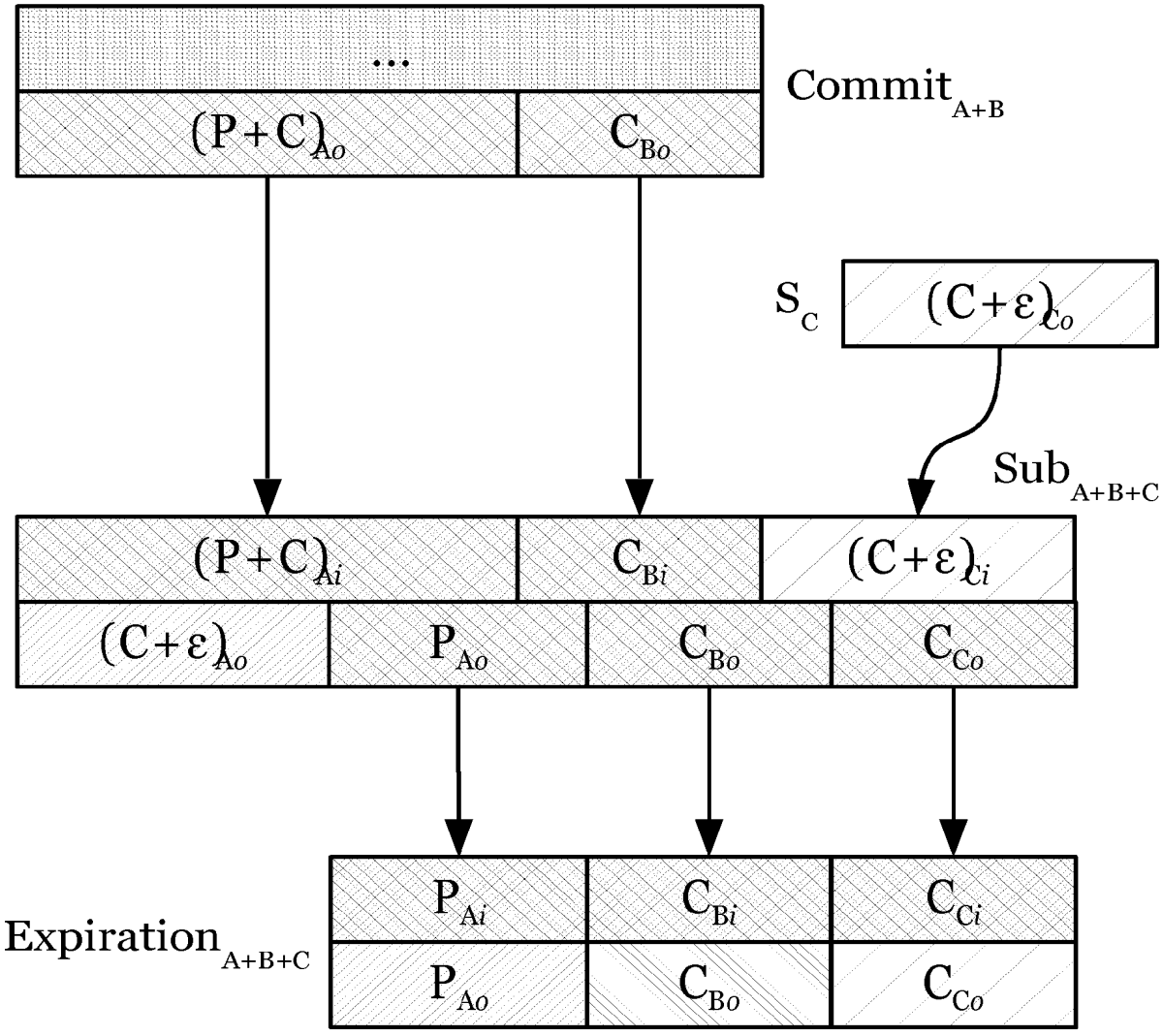

...
$(P+C)_{Ao}$
C_{Bo}
$Commit_{A+B}$
S_C
$(C+\varepsilon)_{Co}$
Sub_{A+B+C}
$(P+C)_{Ai}$
C_{Bi}
$(C+\varepsilon)_{Ci}$
$(C+\varepsilon)_{Ao}$
P_{Ao}
C_{Bo}
C_{Co}
$Expiration_{A+B+C}$
P_{Ai}
C_{Bi}
C_{Ci}
P_{Ao}
C_{Bo}
C_{Co}

FIG. 14

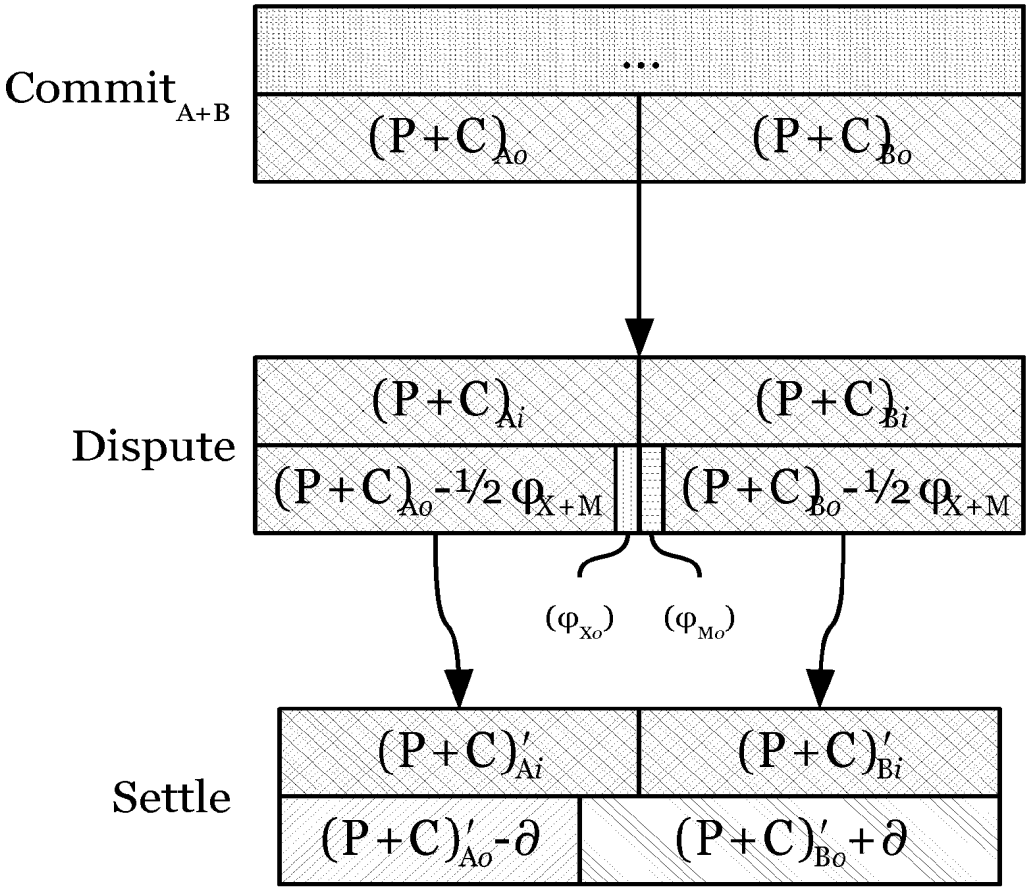

Commit A+B
...
(P+C)Ao
(P+C)Bo
Dispute
(P+C)Ai
(P+C)Bi
(P+C)Ao -½ φX+M
(P+C)Bo -½ φX+M
(φXo)
(φMo)
Settle
(P+C)'Ai
(P+C)'Bi
(P+C)'Ao -∂
(P+C)'Bo +∂

FIG. 15

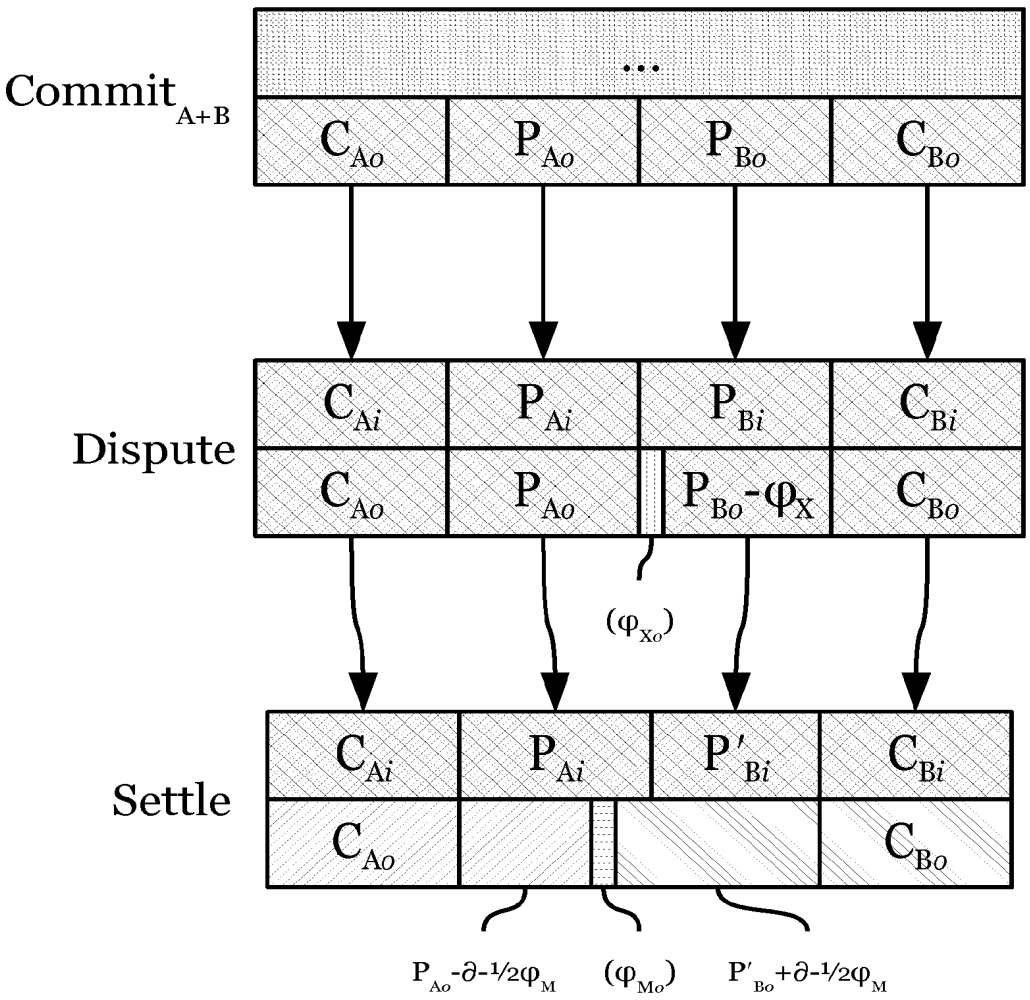

Commit A+B
...
C Ao
P Ao
P Bo
C Bo
Dispute
C Ai
P Ai
P Bi
C Bi
C Ao
P Ao
P Bo -φX
C Bo
(φXo)
Settle
C Ai
P Ai
P′ Bi
C Bi
C Ao
C Bo
PAo-∂-½φM
(φMo)
P′Bo+∂-½φM

FIG. 16

Electronic Acknowledgement Receipt

EFS ID:	18986713
Application Number:	61990795
International Application Number:	
Confirmation Number:	8467
Title of Invention:	SYSTEMS AND METHODS FOR LOW TRUST AND ZERO TRUST TRANSACTIONS
First Named Inventor/Applicant Name:	Reginald C. Middleton
Customer Number:	94276
Filer:	Matthew Thomas Bogosian
Filer Authorized By:	
Attorney Docket Number:	UC-LC-PROV1
Receipt Date:	09-MAY-2014
Filing Date:	
Time Stamp:	11:23:59
Application Type:	Provisional

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$130
RAM confirmation Number	7336
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1		ultracoin_lc_app-20140509.pdf	2835898 fb6f02c208b1e911e232a10790393037fae97871	yes	75

Multipart Description/PDF files in .zip description		
Document Description	**Start**	**End**
Provisional Cover Sheet (SB16)	1	2
Specification	3	54
Claims	55	62
Abstract	63	63
Drawings-only black and white line drawings	64	75

Warnings:

Information:

2	Fee Worksheet (SB06)	fee-info.pdf	29622 6f4f88113a54049f97b970a54cdf6c9166a4f361	no	2

Warnings:

Information:

Total Files Size (in bytes):	2865520

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.

WIPO
WORLD
INTELLECTUAL PROPERTY
ORGANIZATION

DOCUMENT MADE AVAILABLE UNDER THE PATENT COOPERATION TREATY (PCT)

International application number:		**PCT/US2015/029196**
International filing date:		**05 May 2015 (05.05.2015)**
Document type:		**Certified copy of priority document**
Document details:	Country/Office:	**US**
	Number:	**61/990,795**
	Filing date:	**09 May 2014 (09.05.2014)**
Date of receipt at the International Bureau:		**16 May 2015 (16.05.2015)**

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

Electronic Acknowledgement Receipt

EFS ID:	27447829
Application Number:	15309612
International Application Number:	PCT/US15/29196
Confirmation Number:	2321
Title of Invention:	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers
First Named Inventor/Applicant Name:	Reginald Middleton
Customer Number:	115238
Filer:	John Nielsen
Filer Authorized By:	
Attorney Docket Number:	2626.P100.US
Receipt Date:	08-NOV-2016
Filing Date:	
Time Stamp:	14:20:59
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	$960
RAM confirmation Number	110916INTEFSW14252200
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	2626_P100_Transmittal.pdf	491110 ea39e99f5f1f7e36f2c585498dac031ef0397da6	no	3
Warnings:					
Information:					
2	Application Data Sheet	2626_P100_ADS.pdf	498136 d8d9d557faffb5b85d7d67ebecbf2bd03c101383	no	7
Warnings:					
Information:					
This is not an USPTO supplied ADS fillable form					
3	Power of Attorney	2626_P100_POA.pdf	86970 1c084da44633b85c358d824c644436c73d4460f1	no	1
Warnings:					
Information:					
4	Oath or Declaration filed	2626_P100_Inventor_Oaths.pdf	529373 d9c2b0ecdcf7cfe9b103ea4b87dcfb2e44ed5faa	no	4
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	37089 e835161be7efc3bd3cbd96965bef5c00fd1605f0	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1642678		

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.

PTO/SB/01 (09-12)
Approved for use through 01/31/2014. 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 contains a valid OMB control number.

DECLARATION FOR UTILITY OR DESIGN PATENT APPLICATION (37 CFR 1.63)

☒ Declaration Submitted With Initial Filing OR ☐ Declaration Submitted After Initial Filing (surcharge (37 CFR 1.16(f)) required)

Attorney Docket Number	2626.P100.US
First Named Inventor	Reginald Middleton
COMPLETE IF KNOWN	
Application Number	PCT/US 15/29196
Filing Date	11/3/2016
Art Unit	
Examiner Name	

I hereby declare that: (1) Each inventor's residence, mailing address, and citizenship are as stated below next to their name; and (2) I believe the inventor(s) named below to be the original and first inventor(s) of the subject matter which is claimed and for which a patent is sought on the invention titled:

Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers

(Title of the Invention)

the application of which was made or was authorized to be made by me and

☐ is attached hereto

OR

☐ was filed on (MM/DD/YYYY) 05/05/2015 as United States Application Number or PCT International Application Number PCT/US15/29196 and was amended on (MM/DD/YYYY) 11/3/2016 (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified application, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

Authorization To Permit Access To Application by Participating Offices

☒ If 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 World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the above-identified patent application is filed access to the above-identified patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the above-identified patent application is filed to have access to the above-identified patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the above-identified patent application with respect to: 1) the above-identified patent application-as-filed; 2) any foreign application to which the above-identified patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the above-identified patent application; and 3) any U.S. application-as-filed from which benefit is sought in the above-identified patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing the Authorization to Permit Access to Application by Participating Offices.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. 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 21 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/SB/01 (09-12)
Approved for use through 01/31/2014. 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 contains a valid OMB control number.

DECLARATION — Utility or Design Patent Application

Claim of Foreign Priority Benefits

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or (f), or 365(b) of any foreign application(s) for patent, inventor's or plant breeder's rights certificate(s), or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent, inventor's or plant breeder's rights certificate(s), or any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached? YES	NO
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐

☐ Additional foreign application number(s) are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

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.

PTO/SB/01 (09-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

DECLARATION — Utility or Design Patent Application

Direct all correspondence to: ☒ The address associated with Customer Number: 115238 OR ☐ Correspondence address below

Name

Address

City | State | Zip

Country | Telephone | Email

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

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.

NAME OF SOLE OR FIRST INVENTOR: ☐ A petition has been filed for this unsigned inventor

Given Name (first and middle [if any]): Reginald

Family Name or Surname: Middleton

Inventor's Signature: Reginald J. Middleton Date: 11/2/2016

Residence: City: Brooklyn State: NY Country: US Citizenship: USA

Mailing Address: 195 Argyle Road

City: Brooklyn State: NY Zip: 11218 Country: US

☒ Additional inventors or a legal representative are being named on the 1 supplemental sheet(s) PTO/SB/02A or 02LR attached hereto

PTO/SB/02A (07-07)
Approved for use through 01/31/2014. 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 contains a valid OMB control number.

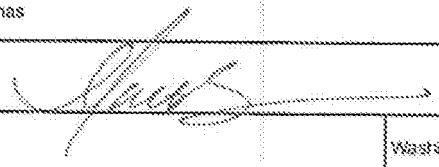
DECLARATION

ADDITIONAL INVENTOR(S)
Supplemental Sheet

Page ____ of ____

Name of Additional Joint Inventor, if any: ☐ A petition has been filed for this unsigned inventor

Given Name (first and middle (if any))	Family Name or Surname
Matthew Thomas	Bogosian

Inventor's Signature  Date 2016-11-01

Residence: City	State	Country	Citizenship
Anacortes	Washington	United States	United States

SSN/ Token (if)

Mailing Address

City	State	Zip	Country
Anacortes	Washington	98221	United States

Name of Additional Joint Inventor, if any: ☐ A petition has been filed for this unsigned inventor

Given Name (first and middle (if any))	Family Name or Surname

Inventor's Signature Date

Residence: City	State	Country	Citizenship

Mailing Address

City	State	Zip	Country

Name of Additional Joint Inventor, if any: ☐ A petition has been filed for this unsigned inventor

Given Name (first and middle (if any))	Family Name or Surname

Inventor's Signature Date

Residence: City	State	Country	Citizenship

Mailing Address

City	State	Zip	Country

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. 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 21 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 (1-800-786-9199) and select option 2.

PCT

REQUEST

The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty.

For receiving Office use only

PCT/US15/29196
International Application No.

05 MAY 2015 (05.05.15)
International Filing Date

PCT INTERNATIONAL APPLICATION RO/US
Name of receiving Office and "PCT International Application"

Applicant's or agent's file reference *(if desired) (12 characters maximum)* 2626.P100.PCT

Box No. I TITLE OF INVENTION

DEVICES, SYSTEMS, AND METHODS FOR FACILITATING LOW TRUST AND ZERO TRUST VALUE TRANSFERS

Box No. II APPLICANT ☐ This person is also inventor

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

VERITASEUM, INC.
195 ARGYLE RD
BROOKLYN NY 11218
US

Telephone No.
1-718-407-4756

Facsimile No.

Applicant's registration No. with the Office

E-mail authorization: Marking one of the check-boxes below authorizes the receiving Office, the International Searching Authority, the International Bureau and the International Preliminary Examining Authority to use the e-mail address indicated in this Box to send, notifications issued in respect of this international application to that e-mail address if those offices are willing to do so.

☒ as advance copies followed by paper notifications; or ☐ exclusively in electronic form (no paper notifications will be sent).

E-mail address: IP@VERITASEUM.COM

State *(that is, country)* of nationality: US

State *(that is, country)* of residence: US

This person is applicant for the purposes of: ☒ all designated States ☐ the States indicated in the Supplemental Box

Box No. III FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)

☒ Further applicants and/or (further) inventors are indicated on a continuation sheet.

Box No. IV 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 ☐ common representative

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

JOHN E. NIELSEN
SENTINEL IP, PC
484 WASHINGTON ST
SUITE B-345
MONTEREY CA 93940
US

Telephone No.
1-510-384-1392

Facsimile No.

Agent's registration No. with the Office
53,392

E-mail authorization: Marking one of the check-boxes below authorizes the receiving Office, the International Searching Authority, the International Bureau and the International Preliminary Examining Authority to use the e-mail address indicated in this Box to send, notifications issued in respect of this international application to that e-mail address if those offices are willing to do so.

☒ as advance copies followed by paper notifications; or ☐ exclusively in electronic form (no paper notifications will be sent).

E-mail address: JOHN@SENTINELPROTECT.US

☐ **Address for correspondence:** Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special address to which correspondence should be sent.

Box No. III FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)

If none of the following sub-boxes is used, this sheet should not be included in the request.

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

REGGINALD MIDDLETON
195 ARGYLE RD
BROOKLYN NY 11218
US

This person is:
- ☐ applicant only
- ☒ applicant and inventor
- ☐ inventor only *(If this check-box is marked, do not fill in below.)*

Applicant's registration No. with the Office

State *(that is, country)* of nationality: US

State *(that is, country)* of residence: US

This person is applicant for the purposes of: ☒ all designated States ☐ the States indicated in the Supplemental Box

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

MATTHEW BOGOSIAN
5007 TOTEM TRL
ANACORTES WA 98221
US

This person is:
- ☐ applicant only
- ☒ applicant and inventor
- ☐ inventor only *(If this check-box is marked, do not fill in below.)*

Applicant's registration No. with the Office: 94,276

State *(that is, country)* of nationality: US

State *(that is, country)* of residence: US

This person is applicant for the purposes of: ☒ all designated States ☐ the States indicated in the Supplemental Box

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

This person is:
- ☐ applicant only
- ☐ applicant and inventor
- ☐ inventor only *(If this check-box is marked, do not fill in below.)*

Applicant's registration No. with the Office

State *(that is, country)* of nationality:

State *(that is, country)* of residence:

This person is applicant for the purposes of: ☐ all designated States ☐ the States indicated in the Supplemental Box

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

This person is:
- ☐ applicant only
- ☐ applicant and inventor
- ☐ inventor only *(If this check-box is marked, do not fill in below.)*

Applicant's registration No. with the Office

State *(that is, country)* of nationality:

State *(that is, country)* of residence:

This person is applicant for the purposes of: ☐ all designated States ☐ the States indicated in the Supplemental Box

☐ Further applicants and/or (further) inventors are indicated on another continuation sheet.

Box No. V DESIGNATIONS

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.

However,

☐ DE Germany **is not designated** for any kind of national protection

☐ JP Japan **is not designated** for any kind of national protection

☐ KR Republic of Korea **is not designated** for any kind of national protection

(The check-boxes above may only be used to exclude (irrevocably) the designations concerned if, at the time of filing or subsequently under Rule 26bis.1, the international application contains in Box No. VI a priority claim to an earlier national application filed in the particular State concerned, in order to avoid the ceasing of the effect, under the national law, of this earlier national application.)

Box No. VI PRIORITY CLAIM AND DOCUMENT

The priority of the following earlier application(s) is hereby claimed:

Filing date of earlier application *(day/month/year)*	Number of earlier application	Where earlier application is:		
		national application: country or Member of WTO	regional application: regional Office	international application: receiving Office
item (1) 09/MAY/2014 09/05/2014	61/990,795	US		
item (2)				
item (3)				

☐ Further priority claims are indicated in the Supplemental Box.

Furnishing the priority document(s):

☒ The **receiving Office** is requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) *(only if the earlier application(s) was filed with the receiving Office which, for the purposes of this international application, is the receiving Office)* identified above as:

☒ all items ☐ item (1) ☐ item (2) ☐ item (3) ☐ other, see Supplemental Box

☐ The **International Bureau** is requested to obtain from a digital library a certified copy of the earlier application(s) identified above, using, where applicable, the access code(s) indicated below *(if the earlier application(s) is available to it from a digital library)*:

☐ item (1) access code _____ ☐ item (2) access code _____ ☐ item (3) access code _____ ☐ other, see Supplemental Box

Restore the right of priority: the receiving Office is requested to restore the right of priority for the earlier application(s) identified above or in the Supplemental Box as item(s) (_____). *(See also the Notes to Box No. VI; further information **must** be provided to support a request to restore the right of priority.)*

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.

Box No. VII INTERNATIONAL SEARCHING AUTHORITY

Choice of International Searching Authority (ISA) *(if more than one International Searching Authority is competent to carry out the international search, indicate the Authority chosen; the two-letter code may be used)*:

ISA/ US

Box No. IX CHECK LIST for EFS-Web filings - this sheet is only to be used when filing an international application with RO/US via **EFS-Web**

This international application **contains** the following:	Number of sheets
(a) request form PCT/RO/101 (including any declarations and supplemental sheets)	4
(b) description (excluding any sequence listing part of the description, see (f), below)	60 ~~59~~ XXX
(c) claims	18
(d) abstract	1
(e) drawings (if any)	16
(f) sequence listing part of the description in the form of an **image file** (e.g. PDF)	
Total number of sheets (including the sequence listing part of the description if **filed as an image file**)	99 ~~98~~ XXX

(g) sequence listing part of the description

- ☐ filed in the form of an **Annex C/ST.25 text file**
- ☐ WILL BE filed separately on physical data carrier(s), on the same day and in the form of an **Annex C/ST.25 text file**

Indicate type and number of physical data carrier(s)

This international application is **accompanied by** the following item(s) *(mark the applicable check-boxes below and indicate in right column the number of each item):*	Number of items
1. ☒ fee calculation sheet	1
2. ☐ original separate power of attorney	
3. ☐ original general power of attorney	
4. ☐ copy of general power of attorney; reference number:	
5. ☐ priority document(s) identified in Box No. VI as item(s)	
6. ☐ Translation of international application into *(language)*:	
7. ☐ separate indications concerning deposited microorganism or other biological material	
8. ☐ *(only where item (f) is marked in the left column)* copy of the sequence listing in electronic form (Annex C/ST.25 text file) not forming part of the international application but **furnished only for the purposes of international search** under Rule 13*ter*	
9. ☐ *(only where item (f) is marked in the left column)* a statement confirming that "the information recorded in electronic form submitted under Rule 13*ter* is identical to the sequence listing as contained in the international application" as filed via EFS-Web:	
10. ☐ copy of results of earlier search(es) (Rule 12*bis*.1(a))	
11. ☐ other *(specify)*:	

Figure of the drawings which should accompany the abstract: 1

Language of filing of the international application: ENGLISH

Box No. X SIGNATURE OF APPLICANT, AGENT OR COMMON REPRESENTATIVE

Next to each signature, indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the request).

JOHN E. NIELSEN
53,392

MAY 1, 2015

05-05-2015

For receiving Office use only

1. Date of actual receipt of the purported international application:	05 MAY 2015
3. Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application:	
4. Date of timely receipt of the required corrections under PCT Article 11(2):	
5. International Searching Authority (if two or more are competent): ISA / US	6. ☐ Transmittal of search copy delayed until search fee is paid

2. Drawings:
- ☐ received:
- ☐ not received:

For International Bureau use only

Date of receipt of the record copy by the International Bureau:

PTO/SB/81 (01-09)
Approved for use through 11/30/2011. 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 OR REVOCATION OF POWER OF ATTORNEY WITH A NEW POWER OF ATTORNEY AND CHANGE OF CORRESPONDENCE ADDRESS

Application Number	PCT/US15/2
Filing Date	5/5/2015
First Named Inventor	Middleton
Title	Devices, Systems, and Methods for Facil...
Art Unit	
Examiner Name	
Attorney Docket Number	2626.P100.US

I hereby revoke all previous powers of attorney given in the above-identified application.

☐ A Power of Attorney is submitted herewith.

OR

☒ I hereby appoint Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith: **115238**

OR

☐ I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

Practitioner(s) Name	Registration Number

Please recognize or change the correspondence address for the above-identified application to:

☐ The address associated with the above-mentioned Customer Number.

OR

☒ The address associated with Customer Number: **115238**

OR

☐ Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the:

☒ Applicant/Inventor.

OR

☐ Assignee of record of the entire interest. See 37 CFR 3.71.
Statement under 37 CFR 3.73(b) (Form PTO/SB/96) submitted herewith or filed on _____.

SIGNATURE of Applicant or Assignee of Record

Signature	Reginald Middleton	Date	11/4/2016
Name	Reginald Middleton	Telephone	718-407-4756
Title and Company	CEO, Veritaseum, Inc.		

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☒ *Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.31, 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.

UTILITY PATENT APPLICATION

DEVICES, SYSTEMS, AND METHODS FOR FACILITATING LOW TRUST AND ZERO TRUST VALUE TRANSFERS

PRIORITY CLAIM

[1] This application claims priority to US provisional application 61/990,795 filed on May, 9, 2014. This application incorporates the disclosures of all applications mentioned in this paragraph by reference as if fully set forth herein.

COPYRIGHT STATEMENT

[2] All material in this document, including the figures, is subject to copyright protections under the laws of the United States and other countries. The owner has no objection to the reproduction of this document or its disclosure as it appears in official governmental records. All other rights are reserved.

TECHNICAL FIELD

[3] Related technical field(s) are: telecommunications, digital communications, and computer technology.

BACKGROUND ART

[4] Overview

[5] Market efficiency tends to increase—and therefore transaction costs tend to decrease—in proportion to the degree that transacting parties trust each other. However, rent extraction tends to increase—and therefore trust decreases—in proportion to market size.[1] Efficient and productive participation in larger markets therefore requires mitigating trust issues, but that comes at a cost. That cost can often be reduced by economies of scale, but even today, there is substantial overhead from buffering against risks introduced by counterparties, intermediaries, post-delivery payment failures, guarantor failures, escrow, etc.

[6] Since the mid 1990s, there has been an explosion of commercial activity where parties previously unknown to each other agree to transact using the internet as the fundamental communication medium, sometimes even across international borders. Establishing and maintaining trust between those parties has played a central role, and various crude solutions based on traditional, but inefficient methods have been attempted (e.g., electronic exchanges

1 Rose, David C. The Moral Foundation of Economic Behavior. New York: Oxford UP, 2011. Print.

with expensive fees, "online" escrow and dispute resolution using third parties, various reputation systems, third party guarantors, etc.).

[7] Among those markets where individuals interact are those which trade financial instruments (e.g., stocks, bonds, options, futures, swaps, currency exposure, etc.). With the advent of financial engineering, individuals and businesses have been able to leverage computing in financial trading, including automating the process of entering and exiting trades based on programmable conditions or algorithms. However, even with the explosion of the use of technology in this space, such technology is overwhelmingly layered on top of legacy centralized markets. Nearly all impose relatively large costs to conduct trades with counterparties. Some very high-volume exchanges sell the ability for "high value" (i.e., high-paying) customers to cut in line ahead of less savvy or less well equipped investors. Some have questioned the fairness of this practice.

[8] Further, the cost of contract enforcement in international trade can be prohibitive, and success might be very difficult to predict. In addition, a seller may wish to receive one currency, and a buyer may wish to send another. The value of one currency denominated in another can be volatile. Historically, one way that remote parties have mitigated risk is to engage the assistance of trusted intermediaries. One such mechanism is a letter of credit (L/C). L/Cs are appropriate where a seller does not know whether to trust a buyer wishing to place a large order, but does trust a bank where the buyer has established a line of credit. The buyer and bank agree that the bank will release funds from that line of credit to the seller when the seller meets certain conditions (most often transmitting evidence of shipment to the bank before a certain date). The bank provides the promise (L/C) to the seller, and the seller and buyer agree on the remaining terms of the transaction. However, payment often happens at a later date than the agreement, and exchange rates could vary between the time that the agreement was struck and the time payment is received. Only the largest of institutions have the resources necessary to properly hedge against exchange rate volatility. Additionally, the fees charged by banks for L/Cs and currency exchanges are substantial. Perversely, a high degree of trust must also be placed in the intermediary institution(s), who effectively acts as self-interested document examiners who may or may not independently verify the veracity of said documents before releasing the funds, perhaps leaving much of the risk of mistake, forgery, or fraud on the shoulders of the seller. As such, L/Cs are typically not well-suited for consumer transactions, or where transactions involve currencies whose values may vary wildly in relation to each other.

[9] Decentralized digital currencies (or so-called "cryptocurrencies")—technologies that promise tightly-controlled asset creation coupled with the ability to transfer control or ownership of those assets computationally when rigorously-defined criteria are met, with little-or-no dependency on third party intermediaries, and with very low transaction costs compared to traditional mechanisms—are relatively new creatures. The Bitcoin protocol and progeny (Ethereum, Litecoin, etc.) are one such class of technologies that have recently enjoyed meteoric rises in popularity (and valuation).

[10] For the purposes of illustration by way of non-limiting example, those particular decentralized digital currencies generally operate by maintaining a whole or partial history or "ledger" (sometimes referred to as a "block chain") of all transactions that have been "validated" by a consensus of network participants. With few exceptions beyond the scope of the invention, transactions function roughly as follows.[2] A transaction comprises at least one input and at least one output. The input comprises an input "script", which comprises an ordered set of well-defined executable operations. The output comprises an output script, which comprises a second ordered set of such operations. A new (child) transaction comprises an input whose input script is combined with the output script from an existing (parent) transaction in a predictable way. The new transaction is considered valid if a majority of network participants agree that the combination, when evaluated according to a predetermined set of rules, produces an anticipated state or result. A transaction output is considered "spent" if it is accepted by a majority of network participants as associated with a valid child transaction. A transaction output is considered "unspent" if, according to a majority of network participants, it is not associated with any valid child transaction. The concept of "ownership" or "title" of a transaction output is determined by which entity may exercise control over said output, or, more specifically, who may create and/or expose new transactions to "spend" said output that will be accepted by a majority of network participants as valid.

[11] More specifically, the entity seeking to submit a new transaction to the ledger transmits (or "broadcasts") a transaction record comprising the details of the desired transaction to a number of network participants then known to the entity (or "peers"). Those peers typically attempt to independently validate the transaction record. If successful, they rebroadcast the transaction record to their peers, and so on. Eventually the transaction record is received by a network participant who is configured to effect the transaction by including the transaction

2 This is an oversimplification of the Bitcoin protocol. More detailed information may be found on the Bitcoin Wiki <https://en.bitcoin.it/>. Details regarding the Ethereum protocol may be found on the Ethereum Wiki <https://github.com/ethereum/wiki/wiki>.

record in the ledger (i.e., in a valid "block"; see more detailed description below).

[12] A transfer occurs when an entity produces a child transaction that is accepted by a majority as valid, and whose input is associated with an unspent output from a parent transaction. In most cases, this is a simple transfer of control to a second entity, where the new transaction's output script is a small set of operations for which creating a corresponding input script is computationally simple for a single entity in possession of a particular asymmetric cryptography key pair, and computationally impractical for all others. In other words, it is "addressed" to an entity with access to a particular private key. Existing software abstracts these addresses and simple transactions sufficiently for laypersons to engage in them without being programmers or protocol experts.

[13] However, many more complex scripts describing conditions under which a transaction may be accepted as valid are contemplated by the set of available operations. Because the general means of describing those operations is typically binary or programming code[3], arbitrary transactions cannot generally be created or understood by laypersons. For example, as of April 21, 2014, the Bitcoin Contracts Wiki page comprises brief instructions for several theoretical "example" transactions.[4] In each, irrespective of role in the transaction, laypersons are unlikely able to understand—much less follow—these instructions. Fundamental steps are missing that would enable them to confidently conduct similar transactions, much less combinations of such transactions. Despite its great potential, this kind of complexity without abstraction has likely frustrated adoption of the Bitcoin protocol and progeny for anything besides "simple" payments in traditional markets.

[14] Decentralized Digital Currencies or "Cryptocurrencies"

[15] The design and functioning of the Bitcoin protocol and progeny can generally be described as follows.[5] While this section often refers to "Bitcoin" by name, the description is accurate for nearly all of the decentralized digital currencies currently known in the art.

[16] Block chain - The "block chain" is a public ledger that records bitcoin transactions. A novel solution accomplishes this without any trusted central authority: maintenance of the block

3 See, e.g., "bitcoind - How Can I Create a Multi Signature 2-of-3 Transaction?" StackExchange, 23 Mar. 2014. Web. 21 Apr. 2014. <https://bitcoin.stackexchange.com/questions/3712/how-can-i-create-a-multi-signature-2-of-3-transaction>.

4 Hearn, Mike. "Contracts." Bitcoin. Bitcoin Community, 9 Apr. 2014. Web. 21 Apr. 2014. <https://en.bitcoin.it/wiki/Contracts>.

5 Adapted from <https://en.wikipedia.org/wiki/Bitcoin> and <https://en.bitcoin.it/wiki/Contracts>.

chain is performed by a network of communicating nodes running bitcoin software. Transactions of the form "payer X sends Y bitcoins to payee Z" are broadcast to this network using readily available software applications. Network nodes can validate transactions, add them to their copy of the ledger, and then broadcast these ledger additions to other nodes. The block chain is a distributed database; in order to independently verify the chain of ownership of any and every bitcoin (amount), each network node stores its own copy of the block chain. Approximately six times per hour, a new group of accepted transactions, a block, is created, added to the block chain, and quickly published to all nodes. This allows bitcoin software to determine when a particular bitcoin amount has been spent, which is necessary in order to prevent double-spending in an environment without central oversight. Whereas a conventional ledger records the transfers of actual bills or promissory notes that exist apart from it, the block chain is the only place that bitcoins can be said to exist in the form of unspent outputs of transactions.

[17] Units - The unit of account of the bitcoin system is bitcoin (BTC). Small multiples of bitcoin used as alternative units are millibitcoin (mBTC), microbitcoin (μBTC), and satoshi. Named in homage to bitcoin's creator, a "satoshi" is the smallest multiple of bitcoin representing 0.00000001 bitcoin, which is one hundred millionth of a bitcoin. A "millibitcoin" equals to 0.001 bitcoin, which is one thousandth of bitcoin. One "microbitcoin" equals to 0.000001 bitcoin, which is one millionth of bitcoin. A microbitcoin is sometimes referred to as a "bit".

[18] Ownership – (See FIG. 24.) Ownership of bitcoins implies that a user can spend bitcoins associated with a specific address. To do so, a payer must digitally sign the transaction using the corresponding private key. Without knowledge of the private key the transaction cannot be signed and bitcoins cannot be spent. The network verifies the signature using the public key. If the private key is lost, the bitcoin network will not recognize any other evidence of ownership; the coins are then unusable, and thus effectively lost. For example, in 2013 one user said he lost 7,500 bitcoins, worth $7.5 million at the time, when he discarded a hard drive containing his private key.

[19] Transactions – Normally, a transaction must have one or more inputs ("coinbase" transactions are special transaction for creating bitcoins and have zero inputs; see "Mining" and "Supply" below). For the transaction to be valid, every input must be an unspent output of a previous transaction. Every input must be digitally signed. The use of multiple inputs corresponds to the use of multiple coins in a cash transaction. A transaction can also have

multiple outputs, allowing one to make multiple payments in one go. A transaction output can be specified as an arbitrary multiple of satoshi. Similarly as in a cash transaction, the sum of inputs (coins used to pay) can exceed the intended sum of payments. In such case, an additional output is used, returning the change back to the payer. Any input satoshis not accounted for in the transaction outputs become the transaction fee.

[20] Every transaction record can have a "lock time" associated with it. This prevents the transaction from being accepted as valid and allows the transaction to be pending and replaceable until an agreed-upon future time. In the case of the Bitcoin and similar protocols, this can be specified either as a block index or as a timestamp. The transaction record will not be accepted for inclusion in the block chain until the transaction's lock time has been reached. Other, more flexible mechanisms have also been proposed[6].

[21] Mining - "Mining" is a record-keeping service. Miners keep the block chain consistent, complete, and unalterable by repeatedly verifying and collecting newly broadcast transactions into a new group of transactions called a "block". A new block contains information that "chains" it to the previous block thus giving the block chain its name. It is a cryptographic hash of the previous block, using the SHA-256 hashing algorithm.

[22] A new block must also contain a so-called "proof-of-work". The proof-of-work consists of a number called a "difficulty target" and a number called a "nonce", which is jargon for "a number used only once". Miners have to find a nonce that yields a hash of the new block numerically smaller than the number provided in the difficulty target. When the new block is created and distributed to the network, every network node can easily verify the proof. On the other hand, finding the proof requires significant work since for a secure cryptographic hash there is only one method to find the requisite nonce: miners try different integer values one at a time, e.g., 1, then 2, then 3, and so on until the requisite output is obtained. The fact that the hash of the new block is smaller than the difficulty target serves as a proof that this tedious work has been done, hence the name "proof-of-work".

[23] The proof-of-work system alongside the chaining of blocks makes modifications of the block chain extremely hard as an attacker must modify all subsequent blocks in order for the modifications of one block to be accepted. As new blocks are mined all the time, the difficulty of modifying a block increases as time passes and the number of subsequent blocks (also called

6 See, e.g., "BIP-65: Revisiting nLockTime" Qntra.net, 13 Nov. 2014. Web. 4 May 2015. <http://qntra.net/2014/11/bip-65-revisiting-nlocktime/>.

"confirmations" of the given block) increases.

[24] Supply - The successful miner finding the new block is rewarded with newly created bitcoins and transaction fees. As of 28 November 2012, the reward amounted to 25 newly created bitcoins per block added to the block chain. To claim the reward, a special transaction called a "coinbase" is included with the processed payments. All bitcoins in circulation can be traced back to such coinbase transactions. The bitcoin protocol specifies that the reward for adding a block will be halved approximately every four years. Eventually, the reward will be removed entirely when an arbitrary limit of 21 million bitcoins is reached c. 2140, and record keeping will then be rewarded by transaction fees solely.

SUMMARY OF INVENTION

[25] The invention pertains to systems and methods enabling parties with little trust or no trust in each other to enter into and enforce agreements conditioned on input from or participation of a third party, over arbitrary distances, without special technical knowledge of the underlying transfer mechanism(s), optionally affording participation of third-party mediators, substitution of transferors and transferees, term substitution, revision, or reformation, etc. Such exchanges can occur reliably without involving costly third-party intermediaries who traditionally may otherwise be required, and without traditional exposure to counterparty risk.

[26] This application explores example embodiments enabling two forms of value transfer: arbitrary swaps and L/Cs. Arbitrary swaps and L/Cs are useful as illustrative examples because traditionally the two are very different animals. However, the invention allows for their expression and enforcement in remarkably similar terms. As one skilled in the art will appreciate, the invention can be applied to many other forms of value transfer as well.

[27] In one example, Party A believes that bitcoins (BTC) will rise in notional terms when valued in New Zealand dollars (NZD) over the next few weeks. Party B believes the opposite is true, that BTC will fall when valued in NZD over a similar timeframe. Neither parties are aware of each other, but each wants to place a small bet in accordance with their respective beliefs. One embodiment of the invention allows those parties to discover each other, collaborate with each other to agree on concrete terms, propose transactions reflecting their agreement, and finally enforce that agreement without traditional, costly measures.

[28] In another example, Party A is a merchant who wishes to allow her customers to trade

their BTC for her services. However, she would rather receive US dollars (USD) because she is concerned about the volatility of BTC. Party A is not concerned about whether BTC will rise or fall when valued in USD. Periodically (e.g., once per day, hour, etc., or even once per transaction where she receives BTC), she can offer to sell exposure to BTC valued in USD in proportion to the BTC she receives from her customers. In other words, she swaps her exposure to BTC in exchange for exposure to USD. Party B has fewer BTC and more USD than he wants, and desires increased exposure to BTC valued in USD. One embodiment of the invention allows Party B to find and exchange—or "swap"—exposures with Party A, allowing Party A to accept BTC in exchange for her goods or services knowing that she will be compensated by Party B if her BTC lose value against USD, in exchange for Party B being able to keep any upside if BTC gains in value against USD. Another embodiment seeks out these swaps automatically upon detection of Party A's ownership of additional BTC.

[29] Combinations are possible. For example, Party A accepts Australian dollars (AUD), but prefers USD, and wants to hedge against volatility of AUD in USD. One embodiment of the invention allows Party A to swap exposure to USD in BTC with Party B, and simultaneously swap exposure to BTC in AUD with Party C over a similar time period, thereby synthesizing a hedge against AUD in USD. The invention is not limited such that Party B and Party C are distinct parties (they could be the same), nor is it limited such that such that Party A must conduct two separate trades. In addition, various embodiments of the invention allow the parties to perform these types of transactions without maintaining currency deposits or making currency purchases or exchanges.

[30] In yet another example, Party A wishes to purchase goods from Party B. The parties do not know each other well. Party B wants assurances of availability of funds from Party A, but Party A does not want to release those funds to Party B (or an assignee) until Party B has demonstrated proof of shipment (or met some other condition)

[31] In one embodiment comprising a swap, a first device called a "client" and a second client participate in a series of transactions where assets (e.g., unspent transaction outputs) from a first party and assets from a second party are committed until a combination of two of the first party, the second party, and an intermediary release them in accordance with a calculation by the intermediary based on observation of external state, such as the relative value of certain financial instruments at a specific time.

[32] In another embodiment comprising a L/C, a first client and a second client participate in a

series of transactions where assets from a first party are committed until either the first client or an intermediary releases them based on observation of external state, such as verification of delivery to a shipper or an address.

[33] In a further embodiment, the assets may be refunded if no such observation can be made by an expiration timestamp.

[34] In yet another embodiment, the commitment of assets may be extended pending a settlement facilitated by a mediator.

BRIEF DESCRIPTION OF THE DRAWINGS

[35] FIG. 1 depicts a typical embodiment for practicing the invention, especially for use with or comprising a transfer mechanism (110) such as a decentralized digital currency (150), where the clients (120, 160, 170), transfer mechanism (110, 150), facilitator (100), and data source (130) are distinct participants connected by a computer network (140).

[36] FIG. 2 depicts aspects of one embodiment pertaining to a swap comprising one or more source transactions and a commit transaction.

[37] FIG. 3 depicts aspects of one embodiment pertaining to a swap comprising a commit transaction and a refund transaction.

[38] FIGS. 4-5 depict aspects of swap embodiments comprising relatively simple disbursement transactions in a swap situation involving principal and collateral.

[39] FIGS. 6-7 depict transaction chains from various example swap embodiments where one party wishes to exit before termination, and cannot secure an agreement from the counterparty, but is able to find a third party willing to stand in place of the party wishing to exit.

[40] FIG. 8 depicts aspects of one embodiment pertaining to a L/C comprising a source transaction and a commit transaction.

[41] FIG. 9 depicts aspects of one embodiment pertaining to a L/C comprising a commit transaction and an expiration transaction.

[42] FIGS. 10-11 depict aspects of L/C embodiments comprising relatively simple disbursement transactions in a situation involving principal and collateral.

[43] FIGS. 12-14 depict transaction chains from various example L/C embodiments comprising

substitutions of parties.

[44] FIGS. 15-16 depict aspects of embodiments where the parties engaged in a value transfer have designated a mediator to resolve any dispute that may arise.

[45] FIGS. 17-22 depict major phases of effecting a value transfer within one embodiment.

[46] FIG. 23 depicts components comprising a typical embodiment of a client or facilitator.

[47] FIG. 24 (prior art) depicts a simplified chain of ownership in a decentralized digital currency.

DESCRIPTION OF THE EMBODIMENTS

[48] The invention is not limited to the following embodiments. The description that follows is for purpose of illustration and not limitation. Other systems, methods, features and advantages will be or will become apparent to one skilled in the art upon examination of the figures and detailed description. It is intended that all such additional systems, methods, features, and advantages be included within this description, be within the scope of the inventive subject matter, and be protected by the accompanying Claims.

[49] For example, the Bitcoin protocol is often used in this application as an illustrative vehicle. However, the invention is not limited by the Bitcoin protocol specifically. Any technology making it sufficiently difficult to recharacterize ownership of assets (virtual or otherwise) unless certain rigorously-defined criteria are met may be substituted. The invention is not limited to decentralized or centralized transfer mechanisms. For example, in one embodiment transactions could be recognized (i.e., facilitated) by an authority (centralized). In another embodiment, they could be validated by election (distributed), etc.

[50] Further, while the Bitcoin protocol and similar technologies explicitly identify "inputs" and "outputs" for transactions, the invention is not limited to such transfer mechanisms. Various embodiments of the invention may be practiced in any context in which ownership of an asset can be recharacterized, provided the transfer mechanism exposes the necessary features. This application uses "input" and "output" both literally (e.g., with respect to technologies like the Bitcoin protocol and progeny) as well figuratively (e.g., with other technologies such as those modeled after double-entry accounting, chain-of-title, etc.). In a more traditional model, for example, an "input" might comprise an amount of some or all of an available "balance" in an "account" under one entity's direction or control (e.g., at a traditional bank). An output might

comprise a reference to another entity's account (e.g., an account number). In such a model, recharacterization of assets occurs when—once certain conditions are met—the balance of the first entity's account is decremented and (preferably atomically) the balance of the second entity's account is incremented. This is but one example of alternative transfer mechanisms with which the invention may be practiced.

[51] In addition, this application may disclose or imply aspects of the invention comprising a "display", a "user input", a "display device", a "user input device", or similar term. However, this invention is not limited to being practiced only by persons with common natural abilities. "Display [device]" is intended to comprise any device capable of unambiguously communicating information to a human being via any of the senses, or combinations of senses. For example, blind persons could use the device with an "audio display", which may comprise a text-to-speech synthesizer. Alternately, a braille terminal could be used. Similarly, "user input [device]" is intended to comprise any device capable of receiving information from a human being. Modernly, popular user input devices comprise a keyboard, a mouse, a touch screen, etc., but could be a speech-to-text converters, sip-and-puff devices, click-and-type devices, motion or gesture recognition devices, etc. These are but a few examples. A diversity of such display and user input devices are known in the art and may be used when practicing the invention, as will become apparent to one skilled in the art.

[52] In the embodiment depicted in FIG. 1, the invention comprises some or all of the depicted participants on a computer network. The participants comprise a first client (A) typically operated for a first party (not depicted) coupled to the computer network (either persistently or intermittently), a second client (B) typically operated for a second party (not depicted) coupled to the computer network (either persistently or intermittently), a transfer mechanism accessible via the computer network, a facilitator accessible to the computer network, and optionally one or more data sources accessible by the facilitator. In a typical embodiment, the computer network comprises the internet and related technologies, but this is not a requirement. Other configurations are possible. For example the computer network could comprise multiple, independent computer networks for connecting any subset of the participants, including private networks, VPNs, secure tunnels, frame relays, etc. Non-limiting modern examples include various standards implemented in hardwire, firmware, or software, and often used in conjunction ("stacked") with each other such as: Ethernet, wireless Ethernet (Wi-Fi), mobile wireless (e.g., CDMA, FDMA, SDMA, TDMA, GSM (GRPS), UMTS, EDGE, LTE, etc.), Bluetooth, Firewire, USB, IP, TCP, UDP, SSL, etc. Any computer networking technology will suffice so long

as it affords communication between the various participants at times consistent with practicing the invention.

[53] In a typical embodiment, each of the first client, the second client, and the facilitator comprises a computer processor configured to perform certain steps within the scope of the invention. In some embodiments, such as those using the Ethereum protocol as the transfer mechanism, the facilitator comprises instructions for computation which are evaluated by network participants in a proof-of-work protocol, in which case a network participant comprises a computer processor configured to evaluate the instructions for computation. In many embodiments, a client comprises a display device and an input device for interacting with a human being, but this is not strictly necessary. In other embodiments, a client could be fully automated, requiring no human intervention. In one such embodiment, the computer processor of the first client is configured to monitor aspects of the transfer mechanism, the facilitator, the data source, the second client, or some other input, and is configured to interact automatically with the various participants based on an observed change of state.

[54] For example, in one embodiment, the transfer mechanism comprises the Bitcoin protocol, and each of the clients, and the facilitator comprises a non-transitory data store for storing key pairs, inchoate transactions, etc. The first client is configured such that when it observes that it acquires new ownership of BTC, it initiates an offer via the facilitator to trade exposure to one financial instrument or asset class (e.g., BTC) in exchange for exposure to another financial instrument or asset class (e.g., USD).

[55] FIG. 1 depicts a typical embodiment for practicing the invention—especially for use with a distributed transfer mechanism—where the clients, transfer mechanism, facilitator, and data source are distinct participants. However, the depicted arrangement is not the only one contemplated by the invention. In an alternate embodiment, the facilitator provides some or all aspects of the transfer mechanism. In another embodiment, the facilitator comprises some or all aspects of a client. For example, part or all of a client's data store, the ability to initiate or accept offers, etc., could be "embedded" in the facilitator, thereby enabling the facilitator to operate as a client itself (e.g., one controlled by the owners of the facilitator, or on behalf of a third party who has entrusted control to the facilitator). In yet another embodiment, the facilitator comprises the data source. Many configurations are contemplated by the invention are possible, and will become apparent to one skilled in the art.

[56] FIG. 2 depicts aspects of one embodiment pertaining to a swap comprising one or more

source transactions and a commit transaction. As depicted, the commit transaction comprises a first input for accepting a first amount from a first source transaction (i.e., from a first party), a second input for accepting a second amount from a second source transaction (i.e., from a second party), and one or more outputs for directing portions of those amounts to one or more other transactions (not depicted), where the first amount and second amount total an expected amount. In many cases, the first and second amounts are equivalent, but not necessarily. In some cases the amounts comprise a principal amount (P), and (optionally) a collateral amount (C), as depicted in the various figures.

[57] In a typical embodiment, the commit transaction is configured such that some or all of the amounts available via its output(s) may only be spent with confirmation from at least two of the first party, the second party, the facilitator, and optionally a third party (such as a mediator). In an alternate embodiment, the commit transaction is configured such that some or all of the amounts available via its outputs may only be transferred with confirmation from one of the facilitator and optionally a trusted third party, and one of the first party and the second party. In another alternate embodiment, the commit transaction is configured such that some or all of the amounts available via its outputs may only be transferred with confirmation from either the facilitator or two of the first party, the second party, and optionally a trusted third party. These are non-limiting examples. In addition to the examples presented herein, commit transactions may be configured such that outputs vest ownership in a conjunction of any number of parties, somewhat analogous to a checking account where checks must be signed by two authorized parties in order to be honored.

[58] While a first source transaction and a second source transaction are depicted in FIG. 2, this should not be construed as a limitation of the invention. Amounts may be input into the commit transaction from any number different sources. Excesses may be refunded back to respective parties, or different parties altogether. The only limitation is that the commit transaction comprises inputs totaling at least the expected amount. In some embodiments, fees (not depicted) may be imposed for directing the amounts from their respective sources to said inputs, which may require adjusting the source transactions to compensate for those fees. For example, transfer mechanisms may impose transfer fees, withdrawal fees, wire fees, etc. The Bitcoin protocol, for example, may require a "mining fee" in order to ensure timely inclusion of the transaction.in the block chain.

[59] FIG. 3 depicts aspects of one embodiment pertaining to a swap comprising a commit

transaction and a refund transaction. The commit transaction comprises a first input for receiving a first principal amount (P_A), a second input for receiving a second principal amount (P_B), and a commit output. The refund transaction comprises an input for receiving an amount from the commit output, a first refund output to the first party, and a second refund output to the second party. In a typical embodiment, a refund transaction record is not created until well after the commit transaction, or it is created such that it is only valid after a certain time in the future and only if the commit output has not yet been spent. This allows another transaction to come before it and spend the commit output, but if no such other transaction is created, the refund transaction record can be submitted to the transfer mechanism to create a refund transaction to put the parties back in or close to their original positions.

[60] FIGS. 4-5 depict aspects of swap embodiments comprising relatively simple disbursement transactions in a swap situation involving principal and collateral. In FIG. 4, the commit transaction comprises a first joined principal and collateral input from a first party and a second joined principal and collateral input from a second party. In FIG. 5, the commit transaction comprises a first principal (P_A) input from a first party, a first collateral (C_A) input from the first party, a second principal (P_B) input from a second party, and a second collateral (C_B) input from the second party. These are but two of many possible configurations that will become apparent to one skilled in the art. For example, a commit transaction could comprise a principal input from a first party, a collateral input from a second party (e.g., a guarantor of the first party, not depicted), and a joined principal and collateral input from a third party.

[61] In the embodiments depicted in FIGS. 4-5, each of the disbursement transactions comprises an input for receiving an amount from the commit output. In FIG. 4, the disbursement transaction comprises a first joined modified principal and collateral disbursement output to the first party, a second joined modified principal and collateral disbursement output to the second party, and an optional fee (φ) output to a third party. In FIG. 5, the disbursement transaction comprises a collateral disbursement output to the first party, a modified principal disbursement output to the first party, a modified collateral disbursement output to the second party, and an optional fee output to a third party. Again, these are but two of many possible configurations that will become apparent to one skilled in the art. For example, analogous to above, a disbursement transaction could comprise a modified principal disbursement output to a first party, a possibly modified (if the principal was exhausted) collateral disbursement output to a third party (e.g., a guarantor of the first party), or a joined modified principal and possibly modified (if the principal was exhausted) disbursement

collateral output to a second party.

[62] In each of the embodiments depicted in FIGS. 4-5, the fee is allocated from the modified principals and is shared equally among the parties to the trade, although this is not required. It could be allocated at any stage, or multiple stages. It could be born solely or disproportionately by one party. Also, in each of the embodiments depicted in FIGS. 4-5, the calculation of the amounts for two or more disbursement outputs comprises a difference (∂), which is positive to one party, and negative to another party. The disbursement transaction in the embodiment depicted in FIG. 5 would be characteristic, for example, of a swap in which the second principal was exhausted before the expiration of the swap, thereby requiring that an amount be allocated from the collateral. In other words, where:

$$\delta > P_B - \frac{1}{2}\varphi \qquad \text{[eq. 1]}$$

[63] To illustrate by way of example how some of the various components above may be used together to facilitate various basic swap agreements, the following steps occur in one embodiment using the Bitcoin or similar protocol as the transfer mechanism, where the parties do not trust each other, and the facilitator is not fully trusted by any of the parties:

1. A first client transmits an offer to a facilitator, the offer comprising terms, the terms comprising:

    a. a reference to a data source comprising at least one of: a base instrument and a quote instrument;

    b. a principal amount;

    c. an expiration timestamp;

    d. optionally a reference to a denominating asset;

    e. optionally, a collateral amount; and

    f. optionally, a disbursement function;

    Example terms:

        Base: USD

Quote: AUD

Denominating: BTC

Principal: 0.5 (BTC)

Collateral: 2 × principal

$res_{base}(b_o, q_o, b_f, q_f)$: $principal \times \frac{b_f - b_o}{q_f - q_o}$

Expiration: 2014-06-01T12:34:56Z

...

2. Optionally, the facilitator validates aspects of the offer (e.g., that the facilitator can interpret the terms, that the expiration timestamp is within an acceptable range, etc.). If validation fails, the facilitator may reject the offer, optionally with an error message to the first client.

3. A second client retrieves the offer from the facilitator.

4. The first client creates a first source transaction record comprising a transaction ID to the transfer mechanism.

5. The second client creates a second source transaction record comprising a transaction ID to the transfer mechanism.

6. The second client transmits the transaction ID of the second source transaction record to the first client, optionally via the facilitator, in such a way that it is associated with the offer (e.g., in the same message, via an offer ID, offer hash, etc.). In another embodiment the first client transmits the transaction ID of the first source transaction record to the second client, and subsequent steps mirror the following of this embodiment.

7. One of the second client and the facilitator transmits a second public key to the first client in such a way that it is associated with the offer.

8. The first client signs (i.e., computes a cryptographic signature and associates it with) a first principal input of an inchoate commit transaction record for creating a complete commit transaction record, the inchoate commit transaction record comprising:

a. the first principal input for receiving a first principal amount from a first source transaction;

b. a second principal input for receiving a second principal amount from a second source transaction; and

c. a commit output comprising a commit amount and a condition requiring signatures of private keys corresponding to two of:

i. a first public key;

ii. the second public key; and

iii. a facilitator public key.

Example inchoate commit transaction record:

```
Input:

      Previous tx: 85e5...e61f

      Index: 1

      scriptSig: efd6...ea1601 a6a6...2c2b

Input:

      Previous tx: 705d...9ce2

      Index: 0

      scriptSig: [sig. placeholder]

...

Output:

      Value: 300000000

      scriptPubKey: 2 67c1...4a70 bf9a...f9e3 cffd...1373 3
      OP_CHECKMULTISIG

...
```

9. The first client transmits the inchoate commit transaction record to the second client, optionally via the facilitator. Optionally, the facilitator validates aspects of the inchoate commit transaction record (e.g., that inchoate commit transaction record is signed by a first party, that the first principal amount and the second principal amount each satisfy the terms, etc.). If validation fails, the facilitator may reject the inchoate commit transaction, optionally with an error message to the first client. Optionally, the facilitator transmits the offer and the inchoate commit transaction record to the second client.

10. Optionally, the second client verifies that the inchoate commit transaction record is as expected, signed by the first party, etc.

11. The second client creates the complete commit transaction record by signing the inchoate commit transaction record and optionally saves a copy in non-transitory memory, the complete commit transaction record comprising:

    a. the first principal input for receiving the first principal amount from the first source transaction;

    b. a second principal input for receiving a second principal amount from the second source transaction; and

    c. a commit output comprising a commit amount and a condition requiring signatures of private keys corresponding to two of:

        i. the first public key;

        ii. the second public key; and

        iii. the facilitator public key.

Example complete commit transaction record:

```
ID: 6b24...b607

Input:

    Previous tx: 85e5...e61f

    Index: 1

    scriptSig: efd6...ea1601 a6a6...2c2b
```

```
Input:

      Previous tx: 705d...9ce2

      Index: 0

      scriptSig: 78eb...fc4501 531f...00dd

...

Output:

      Value: 300000000

      scriptPubKey: 2 67c1...4a70 bf9a...f9e3 cffd...1373 3
      OP_CHECKMULTISIG

...
```

12. The second client signs an inchoate refund transaction record comprising:

a. a lock time after the expiration timestamp;

b. an input for receiving the commit amount from a commit transaction;

c. a first refund output comprising a first refund amount and a first condition requiring approval of the first party; and

d. a second refund output comprising a second refund amount and a condition requiring approval of a second party.

Example inchoate refund transaction record:

```
Input:

      Previous tx: 6b24...b607

      Index: 0

      scriptSig: OP_0 [sig. placeholder] c255...d80301

Output:

      Value: 149995000
```

```
        scriptPubKey: OP_DUP OP_HASH160 53a5...8974 OP_EQUALVERIFY
        OP_CHECKSIG

    Output:

        Value: 149995000

        scriptPubKey: OP_DUP OP_HASH160 30e6...2511 OP_EQUALVERIFY
        OP_CHECKSIG

    ...

    nLockTime: 2014-06-03T12:34:56Z
```

13. The second client transmits the complete commit transaction record and the inchoate refund transaction record to the first client, optionally via the facilitator. Optionally, the facilitator validates aspects of the complete commit transaction record and the inchoate refund transaction record (e.g., that complete refund transaction record is signed by the first party and the second party, that inchoate refund transaction record is signed by the second party, that aspects of the complete commit transaction record match the inchoate commit transaction record, that the first refund amount of the inchoate refund transaction record is not more than the first principal amount, that the second refund amount of the inchoate refund transaction record is not more than the second principal amount, that the lock time is after the expiration timestamp, etc.). If validation fails, the facilitator may reject the inchoate refund transaction record or the complete commit transaction record, optionally with an error message to the second client. Optionally, the facilitator transmits the complete commit transaction record and the inchoate refund transaction record to the first client.

14. Optionally, the first client verifies that the complete commit transaction record is as expected and signed by the first party and the second party, that the inchoate refund transaction record is as expected and is signed by the second party, etc.

15. Optionally, the first client saves a copy of the complete commit transaction record in non-transitory memory.

16. The first client creates a complete refund transaction record and saves a copy in non-transitory memory, the complete refund transaction record comprising:

a. a lock time after the expiration timestamp;

b. an input for receiving the commit amount from the complete commit transaction;

c. a first refund output comprising a first refund amount and a first condition requiring approval of the first party; and

a second refund output comprising a second refund amount and a condition requiring approval of the second party.

Example complete refund transaction record:

```
ID: d5f8...8ab5

Input:

      Previous tx: 6b24...b607

      Index: 0

      scriptSig: OP_0 b859...452c01 c255...d80301

Output:

      Value: 149995000

      scriptPubKey: OP_DUP OP_HASH160 53a5...8974 OP_EQUALVERIFY
      OP_CHECKSIG

Output:

      Value: 149995000

      scriptPubKey: OP_DUP OP_HASH160 30e6...2511 OP_EQUALVERIFY
      OP_CHECKSIG

...

nLockTime: 2014-06-03T12:34:56Z
```

17. The first client transmits the complete refund transaction record to the second client, optionally via the facilitator. Optionally, the facilitator validates aspects of the complete refund transaction record (e.g., that complete refund transaction record is signed by both

the first party, that the complete refund transaction record has not otherwise been modified, is consistent with the terms and the complete commit transaction record, etc.). If validation fails, the facilitator may reject the complete refund transaction record, optionally with an error message to the first client. Optionally, the facilitator transmits the complete refund transaction record to the second client.

18. Optionally, the second client verifies that the complete refund transaction record is as expected and signed by the first party and the second party, etc.

19. After creating or receiving both the complete commit transaction record and the complete refund transaction record, the first client submits the first source transaction record to the transfer mechanism for effecting the first source transaction.

20. After creating or receiving both the complete commit transaction and the complete refund transaction, the second client submits the second source transaction record to the transfer mechanism for effecting the second source transaction.

21. After seeing that both the first source transaction and second source transaction have been submitted to the transfer mechanism, one or both of the first client the second client submit the complete commit transaction record for effecting the commit transaction.

22. On or after the expiration timestamp or at a time or upon an event as defined by the terms, and before the lock time of the complete refund transaction record, the facilitator performs a calculation in accordance with the terms for determining a first disbursement amount and a second disbursement amount, optionally requesting information from one or more data sources for use in the calculation (e.g., the most recent price of a publicly traded financial instrument, the price of the instrument at the time the offer was accepted, etc.). In one embodiment, the data source comprises an external data feed, internal database, another data source, etc.

In the example embodiment, given a time t, the data source provides the value at t of one or more of: the base instrument, the quote instrument, the base instrument in terms of the denominating asset b_t, the quote instrument in terms of the denominating asset q_t, or the base instrument in terms of the quote instrument (e.g., if the base instrument or the quote instrument is also the denominating asset).

In continuing the example above, the base instrument is USD, the quote instrument is AUD, and the denominating asset is BTC. b_o is the value of USD in BTC at the time the trade is initiated. b_f is the value of USD in BTC at the time the trade is completed. q_o is the value of AUD in BTC at the time the trade is initiated. q_f is the value of AUD in BTC at the time the trade is completed. The calculation the facilitator uses to compute the first disbursement amount and the second disbursement amount comprises $res_{base}(b_o, q_o, b_f, q_f)$. In typical embodiments, a party's loss is proportionate to its counterparty's gain, implying:

$$res_{quote}(b_o, q_o, b_f, q_f) = -res_{base}(b_o, q_o, b_f, q_f) \quad \text{[eq. 2]}$$

23. The facilitator signs an inchoate disbursement transaction record, which comprises:

a. an input for receiving the commit amount from the commit transaction;

b. a first disbursement output comprising the first disbursement amount and a first condition requiring approval of the first party;

c. a second disbursement output comprising the second disbursement amount and a condition requiring approval of the second party; and

d. optionally a third disbursement output comprising a fee amount and a condition requiring approval of a third party;

typically where the sum of the first disbursement amount, the second disbursement amount, and any fee amount is not more than the commit amount from the complete commit transaction.

Example inchoate disbursement transaction record:

```
Input:

    Previous tx: 6b24...b607

    Index: 0

    scriptSig: OP_0 [sig. placeholder] ddbb...b00601

Output:
```

```
            Value: 142500736

            scriptPubKey: OP_DUP OP_HASH160 53a5...8974 OP_EQUALVERIFY
            OP_CHECKSIG

      Output:

            Value: 157479264

            scriptPubKey: OP_DUP OP_HASH160 30e6...2511 OP_EQUALVERIFY
            OP_CHECKSIG

      Output:

            Value: 10000

            scriptPubKey: OP_DUP OP_HASH160 d377...5c8c OP_EQUALVERIFY
            OP_CHECKSIG

      ...
```

24. The facilitator transmits the inchoate disbursement transaction record to both the first client and the second client, either of whom may independently verify, sign, and submit the disbursement transaction record to the transfer mechanism before the time arrives that the other can successfully submit the complete refund transaction record.

[64] The above is but one embodiment of a vale transfer according to the invention. In another, equivalent or alternate steps may be used. The following describes an embodiment comprising an atypical, but illustrative arrangement:

1. A first client transmits an offer to a second client.

2. The first client transmits the offer to a facilitator.

3. The facilitator transmits to the first client a first inchoate commit transaction record for creating a complete commit transaction record, the first inchoate commit transaction record comprising:

    a. a first principal input for receiving a first principal amount from a first source transaction; and

    b. a first commit output comprising a first commit amount and a condition

requiring approval of two of:

i. a first party;

ii. a second party; and

iii. the facilitator.

4. The facilitator transmits to the second client a second inchoate commit transaction record for creating the complete commit transaction record, the second inchoate commit transaction record comprising:

a. a second principal input for receiving a second principal amount from a second source transaction; and

b. a second commit output comprising a second commit amount and a condition requiring approval of two of:

i. the first party;

ii. the second party; and

iii. the facilitator.

5. The first client signs a first source transaction record.

6. The first client completes and signs (e.g., with `SIGHASH_SINGLE | SIGHASH_ANYONECANPAY`) the first inchoate commit transaction record.

Example first inchoate commit transaction record:

```
...
Input:
      Previous tx: 85e5...e61f
      Index: 1
      scriptSig: 5e7c...a11a83 ecad...d0ba
...
```

```
Output:

      Value: 150000000

      scriptPubKey: 2 67c1...4a70 bf9a...f9e3 cffd...1373 3
      OP_CHECKMULTISIG

...
```

7. The first client transmits the first inchoate commit transaction record to the facilitator.

8. The second client signs a second source transaction record.

9. The second client completes and signs (e.g., with `SIGHASH_SINGLE | SIGHASH_ANYONECANPAY`) the second inchoate commit transaction record.

Example second inchoate commit transaction record:

```
...

Input:

      Previous tx: 705d...9ce2

      Index: 0

      scriptSig: ade1...9dcb83 f058...878a

...

Output:

      Value: 150000000

      scriptPubKey: 2 67c1...4a70 bf9a...f9e3 cffd...1373 3
      OP_CHECKMULTISIG

...
```

10. The second client transmits the second inchoate commit transaction record to the facilitator.

11. The facilitator creates the complete commit transaction record from the first inchoate transaction record and the second inchoate commit transaction record, the complete

commit transaction record comprising:

a. a first principal input for receiving a first principal amount from the first source transaction; and

b. a first commit output comprising a first commit amount and a condition requiring approval of two of:

   i. the first party;

   ii. the second party; and

   iii. the facilitator;

c. a second principal input for receiving a second principal amount from the second source transaction; and

d. a second commit output comprising a second commit amount and a condition requiring approval of two of:

   i. the first party;

   ii. the second party; and

   iii. the facilitator.

Example complete commit transaction record:

```
ID: 11f0...8ea8

Input:

      Previous tx: 85e5...e61f

      Index: 1

      scriptSig: 5e7c...a11a83 ecad...d0ba

Input:

      Previous tx: 705d...9ce2

      Index: 0
```

```
        scriptSig: ade1...9dcb83 f058...878a

    ...

    Output:

        Value: 150000000

        scriptPubKey: 2 67c1...4a70 bf9a...f9e3 cffd...1373 3
        OP_CHECKMULTISIG

    Output:

        Value: 150000000

        scriptPubKey: 2 67c1...4a70 bf9a...f9e3 cffd...1373 3
        OP_CHECKMULTISIG

    ...
```

In another embodiment, the first client provides a transaction ID of the first source transaction record to the facilitator and the second client provides a transaction ID of the second source transaction record to the facilitator before the facilitator transmits the first inchoate commit transaction record and the second inchoate commit transaction record. The facilitator creates the first inchoate commit transaction record identical to the second inchoate commit transaction record, each comprising a first principal input with a placeholder signature and a second principal input with a placeholder signature. Once the respective inchoate commit transaction records are transmitted to the respective clients, the clients each sign their respective principal input (e.g., with `SIGHASH_ALL | SIGHASH_ANYONECANPAY`) before returning their respective signed inchoate commit transaction record back to the facilitator. The facilitator collects the signed inchoate commit transaction records and consolidates the signed inputs into a complete commit transaction record. In such an embodiment, the first commit output and the second commit output could be consolidated, and the corresponding disbursement transaction record and refund transaction record could omit their respective second inputs.

12. The facilitator transmits the completed commit transaction record to the first client who optionally stores it in non-transitory memory.

13. The facilitator transmits the completed commit transaction record to the second client who optionally stores it in non-transitory memory.

14. The first client signs (e.g., `SIGHASH_ALL | SIGHASH_ANYONECANPAY` or `SIGHASH_SINGLE | SIGHASH_ANYONECANPAY`) an inchoate refund transaction record comprising:

    a. a lock time after the expiration timestamp;

    b. a first input for receiving the first commit amount from a commit transaction;

    c. a second input for receiving the second commit amount from the commit transaction;

    d. a first refund output comprising a first refund amount and a first condition requiring approval of the first party; and

    e. a second refund output comprising a second refund amount and a second condition requiring approval of the second party.

    Example inchoate refund transaction record:

```
Input:
        Previous tx: 11f0...8ea8
        Index: 0
        scriptSig: OP_0 78a2...203181 [sig. placeholder]
Input:
        Previous tx: 11f0...8ea8
        Index: 1
        scriptSig: OP_0 fdbe...893f81 [sig. placeholder]
...
Output:
        Value: 149995000
```

```
        scriptPubKey: OP_DUP OP_HASH160 53a5...8974 OP_EQUALVERIFY
        OP_CHECKSIG

    Output:

        Value: 149995000

        scriptPubKey: OP_DUP OP_HASH160 30e6...2511 OP_EQUALVERIFY
        OP_CHECKSIG

    ...

    nLockTime: 2014-06-03T12:34:56Z
```

15. The first client transmits the complete commit transaction record and the inchoate refund transaction record to the second client.

16. The second client creates the complete refund transaction record from the inchoate refund transaction record (e.g., signing with `SIGHASH_ALL | SIGHASH_ANYONECANPAY` or `SIGHASH_SINGLE | SIGHASH_ANYONECANPAY`) and saves a copy in non-transitory memory.

    Example complete refund transaction record:

```
    ID: eb09...3d15

    Input:

        Previous tx: 11f0...8ea8

        Index: 0

        scriptSig: OP_0 78a2...203181 b765...fc4383

    Input:

        Previous tx: 11f0...8ea8

        Index: 1

        scriptSig: OP_0 fdbe...893f81 91e4...4dd583

    ...
```

```
Output:

      Value: 149995000

      scriptPubKey: OP_DUP OP_HASH160 53a5...8974 OP_EQUALVERIFY
      OP_CHECKSIG

Output:

      Value: 149995000

      scriptPubKey: OP_DUP OP_HASH160 30e6...2511 OP_EQUALVERIFY
      OP_CHECKSIG

...

nLockTime: 2014-06-03T12:34:56Z
```

17. The second client transmits the complete refund transaction record to the first client.

18. After creating or receiving both the complete commit transaction record and the complete refund transaction record, the first client submits the first source transaction record to the transfer mechanism.

19. After creating or receiving both the complete commit transaction record and the complete refund transaction record, the second client submits the second source transaction record to the transfer mechanism.

20. After seeing that both the first source transaction record and second source transaction record have been submitted, one or both of the first client the second client submits the complete commit transaction record.

21. On or after the expiration timestamp, or at a time or upon an event as defined by the terms, and before the lock time of the complete refund transaction record, the facilitator performs a calculation in accordance with the terms for determining a first disbursement amount and a second disbursement amount, optionally requesting information from one or more data sources for use in the calculation.

22. The facilitator signs an inchoate disbursement transaction record (e.g., signing with `SIGHASH_ALL | SIGHASH_ANYONECANPAY` or `SIGHASH_SINGLE | SIGHASH_ANYONECANPAY`).

Example inchoate disbursement transaction record:

```
Input:

      Previous tx: 11f0...8ea8

      Index: 0

      scriptSig: OP_0 [sig. placeholder] 8cd3...d86481

Input:

      Previous tx: 11f0...8ea8

      Index: 1

      scriptSig: OP_0 [sig. placeholder] 12bc...825281

...

Output:

      Value: 142500736

      scriptPubKey: OP_DUP OP_HASH160 53a5...8974 OP_EQUALVERIFY
      OP_CHECKSIG

Output:

      Value: 157479264

      scriptPubKey: OP_DUP OP_HASH160 30e6...2511 OP_EQUALVERIFY
      OP_CHECKSIG

Output:

      Value: 10000

      scriptPubKey: OP_DUP OP_HASH160 d377...5c8c OP_EQUALVERIFY
      OP_CHECKSIG

...
```

23. The facilitator transmits the inchoate disbursement transaction record to both the first client and the second client, either of whom can submit it as in the prior example

embodiment.

[65] Various verification steps have been omitted for brevity.

[66] It will become apparent to one skilled in the art that aspects of each of embodiments above may be commingled. For example, the first client could transmit the offer to the facilitator, where the second client could find and retrieve it. As mentioned above, aspects of one or both of the first client and the second client could coincide with the facilitator allowing many of the above steps to be omitted as redundant where the facilitator is entrusted to act as a proxy for or on behalf of one of the first party and the second party. The facilitator could contain aspects of one of the clients, but not the other, in which case the extra-facilitator client would optionally independently validate transaction records it received from the facilitator before signing them, etc. In such embodiments, the facilitator typically comprises a means to control aspects of a client it comprises via an interface such as a web-based user interface (UI), an application programmer's interface (API), etc.

[67] In such embodiments, any party delegating authority to the facilitator must trust the facilitator to be secure and to act fairly, but these are similar to expectations many parties already have of traditional third party intermediaries. Assuming the first party has independent access to same key pairs the facilitator uses to act on behalf of the first party, and the second party has independent access to the same key pairs the facilitator uses to act on behalf of the second party, even if the facilitator is destroyed, both the first party and the second party may retrieve their assets, at worst by submitting any complete refund transaction record to the transfer mechanism on or after the lock time, assuming they have kept copies of the complete refund transaction record in their respective non-transitory memories.

[68] In one embodiment, a client is configured such that when it detects a new spendable output comprising an amount (e.g., by monitoring changes in or updates to the block chain when using the Bitcoin or similar protocol as the transfer mechanism), it automatically accepts a remote offer comprising an amount compatible with the amount of the new spendable output. If no such remote offer is available, it transmits an offer comprising an amount substantially similar to the new spendable output (e.g., to the facilitator, to another client, etc.). In another embodiment, when the client detects a second new spendable output, it attempts to rescind the offer. If successful, it transmits a new offer comprising an amount which comprises some or all of the new spendable output and some or all of the second new spendable output. Other variations are possible. For example, the client could be configured to scan available offers and

match the available offers to the amounts of the spendable outputs. Matching algorithms vary in complexity and are known in the art. For example, many Bitcoin protocol client implementations provide such algorithms for matching spendable outputs to the inputs of simple transactions. Such algorithms are adaptable by those of ordinary skill in the art for this and similar embodiments of the invention.

[69] In various embodiments, the terms comprise a ratio of a first instrument to a second instrument, optionally denominated in an asset, as well as an amount that each participant must allocate. For example, in one embodiment, the terms could offer to "sell" 2 BTC/USD with a required allocation of 3 BTC from each party. In other words, the swap defined by the terms offers exposure to 2 BTC of USD, and each participant must allocate 2 BTC to principal and 1 BTC to collateral for the duration of the swap (i.e., until it expires, or until the principal and collateral of one party is exhausted).

[70] The allocations for each party need not be equal. In one embodiment, if the market expects a particular instrument pair to decline over the life of the swap, the party accepting exposure to that instrument pair may be required to allocate more collateral than the counterparty. Note that in the previous example, the parties' risk formulas are asymmetric. The most the offeror could lose is the principal of 2 BTC (if BTC become worthless when valued in USD). However, the offeree's losses are unbounded (if USD becomes worthless when valued in BTC). In other words:

$$res_{base}(b_o, q_o, b_f, q_f) = principal \times \frac{b_f - b_o}{q_f - q_o} \quad \text{[eq. 3]}$$

[71] Alternately:

$$res_{base}(b_o, q_o, b_f, q_f) = principal \times \left(\frac{b_f}{q_f} - \frac{b_o}{q_o} \right) \quad \text{[eq. 4]}$$

[72] In other embodiments symmetrical models could be adopted. Consider:

$$res_{base}(b_o, q_o, b_f, q_f) = \begin{cases} \frac{b_t}{q_f} \leq \frac{b_o}{q_o} & : \quad principal \times \left(\frac{b_f q_o}{b_o q_f} - 1 \right) \\ \frac{b_t}{q_f} > \frac{b_o}{q_o} & : \quad principal \times \left(1 - \frac{b_o q_f}{b_f q_o} \right) \end{cases} \quad \text{[eq. 5]}$$

[73] Where $res_{base}(...)$ is the resulting gain or loss to the party taking the base instrument exposure at time f given the initial value of the base instrument b_o, the initial value of the quote instrument q_o, the value of the base instrument b_f at time f, and the value of the quote instrument q_f at time f. The resulting gain or loss for the party taking the quote instrument exposure is inverted:

$$\begin{aligned} res_{quote}(b_o, q_o, b_f, q_f) &= -res_{base}(b_o, q_o, b_f, q_f) \\ &= \begin{cases} \frac{b_f}{q_f} \le \frac{b_o}{q_o} & : \quad principal \times \left(1 - \frac{b_f q_o}{b_o q_f}\right) \\ \frac{b_f}{q_f} > \frac{b_o}{q_o} & : \quad principal \times \left(\frac{b_o q_f}{b_f q_o} - 1\right) \end{cases} \end{aligned} \qquad \text{[eq. 6]}$$

[74] In this embodiment, the parties' risk formulas are symmetric. If the base instrument goes to zero, the most the party taking the base instrument exposure can lose is the principal. Likewise, if the quote instrument goes to zero, the most the party taking the quote instrument exposure can lose is the principal. Note that no collateral is needed. Alternately, consider:

$$\begin{aligned} res_{base}(b_o, q_o, b_f, q_f) &= -res_{quote}(b_o, q_o, b_f, q_f) \\ &= \begin{cases} \frac{b_f}{q_f} \le \frac{b_o}{q_o} & : \quad -principal \times \frac{b_o q_f}{b_f q_o} \\ \frac{b_f}{q_f} > \frac{b_o}{q_o} & : \quad principal \times \frac{b_f q_o}{b_o q_f} \end{cases} \end{aligned} \qquad \text{[eq. 7]}$$

[75] In this embodiment, the parties' risk formulas are also symmetric. However, as the base instrument goes to zero, the loss incurred by the party taking the base instrument approaches infinity, all else being equal. Likewise, as the quote instrument goes to zero, the loss incurred by the party taking the quote instrument position approaches infinity, all else being equal. Note that collateral is needed when losses exceed principal amounts. The more volatile the instrument pair, the more collateral may be required to minimize risk of termination before expiration. These are but a few basic examples. Terms affecting the calculation for determining the allocation disbursement amounts can be arbitrarily complex and are limited by the imaginations of the participants. All such variations are contemplated by the invention.

[76] In some circumstances, a party may wish to exit a value transfer (e.g., a swap) before it expires. The parties may agree to terminate prematurely. In one embodiment, the facilitator

facilitates this by creating the inchoate disbursement transaction record as if the swap had expired when the parties agreed to exit. The requesting party signs the inchoate disbursement transaction record and transmits it to the acquiescing party who signs and submits it to the transfer mechanism. Optionally, if the facilitator includes a fee output to a third party, the acquiescing party may require that the fee would be born disproportionately, or entirely by the requesting party.

[77] Where one party wishes to exit before termination, but cannot secure an agreement from the counterparty, another option is for the party seeking premature termination to find a third party substitute. FIGS. 6-7 depict transaction chains from various example swap embodiments comprising such substitutions.

[78] FIG. 6 depicts aspects of an embodiment where a withdrawing party (A) has convinced an entering party (C) to substitute into a value transfer with a remaining party (B). In addition, the entering party transfers a negotiated amount (ε) to the withdrawing party. This is facilitated in the depicted embodiment by a substitution transaction, a second commit transaction, and a second refund transaction.

[79] For clarity of illustration, the outputs of the commit transaction and the corresponding inputs of the substitution transaction are depicted as separate for each of the first principal (P_A), the first collateral (C_A), the second principal (P_B), and the second collateral (C_B). This is not a limitation of the invention. Just as with the previously described embodiments, the outputs of the commit transaction, and corresponding inputs of the substitution transaction could be any configuration considered valid by the transfer mechanism. The outputs of the substitution transaction and inputs to the second commit transaction are similarly depicted for clarity of illustration. Again, all valid configurations of inputs and outputs between transactions are contemplated by the invention.

[80] A difference (∂) used to calculate the first disbursement amount and the second disbursement amount as if the transaction had expired at the time of the substitution. In the embodiment depicted in FIG. 6, this favors the remaining party. Therefore, the substitution transaction record is constructed such that the withdrawing party takes a loss in proportion to that difference, and the entering party need only provide assets to cover the remaining position.

[81] Also, in the embodiment depicted in FIG. 6, the substitute refund is asymmetric. The entering party is refunded what that party committed to the transaction (less the negotiated

amount), and the remaining party is refunded what that party would have received had the swap expired at the time of substitution. Other variations are possible. For example, in one embodiment, the negotiated amount may be transferred separately, at another phase of the value transfer, or in a separate value transfer altogether.

[82] In the embodiment depicted in FIG. 7, the substitution favors the withdrawing party. In that embodiment, the substitute refund is symmetric. The remaining party is refunded what that party would have received had the original transaction been refunded.

[83] In one embodiment, a substitution is facilitated by the following steps:

1. The facilitator performs a calculation in accordance with the terms for determining a withdrawal amount and an entry amount, optionally requesting information from one or more data sources for use in the calculation.

2. The facilitator creates an inchoate substitution transaction record comprising:

    a. a first input for receiving an amount from a commit transaction;

    b. an entry input for receiving the entry amount from a source transaction;

    c. a withdrawal output comprising the withdrawal amount and a first condition requiring approval of the first party; and

    d. a substitution output comprising a substitution amount and a second condition requiring approval of two of:

        i. the second party;

        ii. the third party; and

        iii. the facilitator.

Example inchoate substitution transaction record:

```
Input:

    Previous tx: 6b24...b607

    Index: 0
```

```
            scriptSig: OP_0 [sig. placeholder] [sig. placeholder]
      Input:
            Previous tx: dd66...ae8e
            Index: 3
            scriptSig: [sig. placeholder]
      Output:
            Value: 300000000
            scriptPubKey: 2 bf9a...f9e3 952b...0542 cffd...1373 3
            OP_CHECKMULTISIG
      Output:
            Value: 121871000
            scriptPubKey: OP_DUP OP_HASH160 6250...6cfc OP_EQUALVERIFY
            OP_CHECKSIG
      ...
```

3. The facilitator transmits the inchoate substitution transaction record to the first party and the third party.

4. The first party creates a first signed inchoate substitution transaction record by signing the first input of inchoate substitution transaction record (e.g., signing with `SIGHASH_ALL | SIGHASH_ANYONECANPAY`) and transmits the first signed inchoate substitution transaction record to the facilitator.

5. The third party creates a second signed inchoate substitution transaction record by signing the entry input of the inchoate substitution transaction record (e.g., signing with `SIGHASH_ALL | SIGHASH_ANYONECANPAY`) and transmits the second signed inchoate substitution transaction record to the facilitator.

6. The facilitator creates a complete substitution transaction record (e.g., `ID: 9c8b...4794`) from the first inchoate substitution transaction record and the second inchoate substitution transaction record.

7. The facilitator signs an inchoate substitute refund transaction record comprising:

   a. a lock time after the expiration timestamp;

   b. an input for receiving the substitution amount from a substitution transaction;

   c. a first refund output comprising a first refund amount and a first condition requiring approval of the second party; and

   d. a second refund output comprising a second refund amount and a condition requiring approval of the third party.

   Example inchoate substitute refund transaction record:

```
Input:

      Previous tx: 9c8b...4794

      Index: 0

      scriptSig: OP_0 [sig. placeholder] b2ac...8a4601

Output:

      Value: 178124000

      scriptPubKey: OP_DUP OP_HASH160 30e6...2511 OP_EQUALVERIFY
      OP_CHECKSIG

Output:

      Value: 121866000

      scriptPubKey: OP_DUP OP_HASH160 94e2...4fb6 OP_EQUALVERIFY
      OP_CHECKSIG

...

nLockTime: 2014-06-03T12:34:56Z
```

8. The facilitator creates a signed substitute refund transaction record by signing the inchoate substitute refund transaction record and transmits the signed substitute refund transaction record to the second party and the third party.

9. The facilitator submits the complete substitution transaction record to the transfer mechanism.

[84] Various verification and details steps disclosed in previous embodiments have been omitted for brevity. In other embodiments, the various transaction records are created or signed by the first party or the second party instead of the facilitator. For example, the first party and the second party could agree upon the amounts in the substitution transaction record, and each could sign it without involving the facilitator. All such variations are considered part of the invention.

[85] A letter of credit (L/C) is well known in the art, but is fundamentally an agreement where a third party transfers assets to a second party on behalf of a first party upon some agreed upon condition being demonstrated as met before an agreed upon time (an expiration). Typically, this comprises an expensive manual review of arcane shipping documents by an intermediary financial institution before it will release funds on behalf of a buyer. However this costly approach can be eschewed in favor of one embodiment of the invention in which the facilitator conditions the creation and transmission of a disbursement transaction record based on the result from a query to a shipper's public API regarding a known tracking number. In other embodiments, L/C terms comprise evaluating search results, observation of the presence or absence of data at an anticipated location, checking that the value of a variable or response from an API is within a set of expected values or matches an anticipated pattern, receiving a signal from a digital instrument (e.g., a temperature sensor, a GPS, etc.) and validating that a signal value is within an anticipated range or tolerance, etc. The possibilities are many and varied. For example, US continuation application 13/970,755 ('755) describes systems and methods for efficiently calculating geospatial nearness. Others are known in the art. In one embodiment, the calculation comprises a condition whereupon an object is or was "at" or "near" (i.e., within a specified distance of) a particular location. Mechanisms to discover the location of said object are known in the art (e.g., self-reporting GPSs, Automatic Identification and Data Capture (AIDC) devices, such as barcodes, Quick Response (QR) Codes, Radio Frequency Identification (RFID) tags, in proximity of a reporting detector or sensor at a known location, etc.). Many possible configurations are contemplated by the invention, and will become apparent to one skilled in the art.

[86] FIG. 8 depicts aspects of one embodiment pertaining to a L/C comprising a source transaction and a commit transaction. As depicted, the commit transaction comprises a first

input for accepting a first amount from a first source transaction (i.e., from a first party), and one or more outputs for directing a portion of the first amount to one or more other transactions (not depicted). In other embodiments (portions of which are depicted in other figures), the commit transaction further comprises a second input for accepting a second amount from a second source transaction (i.e., from a second party), where the first amount and second amount total an expected amount. In some cases the amounts comprise a principal amount (P), and (optionally) a collateral amount (C), as depicted in the various figures. While only a first source transaction is depicted in FIG. 8, that should not be construed as a limitation of the invention.

[87] FIG. 9 depicts aspects of one embodiment pertaining to a L/C comprising a commit transaction and an expiration transaction, the expiration transaction being analogous to the refund transaction in previously described embodiments. However, where a refund transaction is meant exclusively for recovery of funds in the event of an exception (e.g., the facilitator becomes unavailable to create or sign a disbursement transaction record), use of an expiration transaction, in addition to recovery, is contemplated by the offer (e.g., if the conditions set forth are not satisfied before the expiration timestamp, despite the facilitator being operational). The difference is largely conceptual. The two function almost identically within the invention. The commit transaction comprises a first input for receiving a first principal amount (P_A), and a commit output. The expiration transaction comprises an input for receiving an amount from the commit output, a first expiration output to the first party. In other embodiments where the commit transaction comprises a second input for receiving a second amount, the expiration transaction comprises a second expiration output to the second party.

[88] FIGS. 10-11 depict aspects of L/C embodiments comprising relatively simple disbursement transactions in a situation involving principal and collateral. In FIG. 10, the commit transaction comprises a first joined principal and collateral ($(P+C)_A$) input from a first party. In other embodiments, just as with those mentioned above, the inputs need not be joined. In FIG. 11, the commit transaction comprises a first joined principal and collateral input from a first party, and a second collateral (C_B) input from the second party. These are but two of many possible configurations contemplated by the invention. For example, a commit transaction could comprise a principal input from a first party, a collateral input from a third party (e.g., a guarantor of the first party, not depicted), and a collateral input from a second party.

[89] In the embodiments depicted in FIGS. 10-11, each of the disbursement transactions comprises an input for receiving an amount from the commit output. In FIG. 10, the

disbursement transaction comprises a first collateral disbursement output to the first party, a first principal disbursement output to the second party, and an optional fee (φ) output to a third party, where the fee is deducted from the collateral. In FIG. 11, the disbursement transaction comprises a collateral disbursement output to the first party, and a joined principal and collateral disbursement output to the second party. In addition, the commit transaction comprises an optional fee output to a third party, which is born equally by the parties in the disbursement transaction. Again, these are but two of many possible configurations contemplated by the invention. For example, the optional fee output could be allocated at any stage, or multiple stages. It could be born solely or disproportionately by one party at the same or different stages.

[90] To illustrate by way of example how some of the various components above may be used together to facilitate various L/C agreements, the following steps occur in one embodiment using the Bitcoin or similar protocol as the transfer mechanism, where the parties do not trust each other, and the facilitator is not fully trusted by any of the parties:

1. A first client creates an offer, the offer comprising terms, the terms comprising:

    a. one of a disbursement condition comprising one or more references to a data source, a reference to a disbursement condition comprising one or more references to a data source, a disbursement function comprising one or more references to a data source, and one or more references to a disbursement function comprising one or more reference to a data source;

    b. a principal amount;

    c. an expiration timestamp;

    d. optionally, a first collateral amount; and

    e. optionally, a second collateral amount.

    Example terms:

        Payer principal: 0.5 (BTC)

        Payer collateral: 1 × principal

        Payee collateral: 0.05 × principal

Disbursement condition:

```
FedEx("987654321").deliveredToCarrier() == true
```

Expiration: 2014-06-01T12:34:56Z

...

2. The first client signs a first source transaction record.

3. The first client creates an inchoate commit transaction record comprising:

   a. the first input for receiving the first amount from a first source transaction;

   b. optionally, a second input for receiving a second amount from a second source transaction;

   c. a commit output comprising a commit amount and a condition requiring approval of two of:

      i. a first party;

      ii. a second party; and

      iii. a facilitator.

4. Optionally, the first client transmits the offer to the facilitator, who validates aspects of the offer (e.g., that the facilitator can interpret the terms, that the expiration timestamp is within an acceptable range, etc.). If validation fails, the facilitator may reject the offer, optionally with an error message to the first client.

5. The first client transmits the offer to a second client.

6. Optionally, if the inchoate commit transaction record comprises a second input, the first client transmits the inchoate commit transaction record to the second client. The second client signs a second source transaction record. The second client signs the inchoate commit transaction record. The second client transmits the signed inchoate commit transaction record back to the first client.

7. The first client creates a complete commit transaction record by signing (e.g., with `SIGHASH_ALL | SIGHASH_ANYONECANPAY`) the inchoate commit transaction record,

optionally storing the complete commit transaction record in non-transitory memory.

Example complete commit transaction record:

```
ID: c215...fc9b

Input:

      Previous tx: 85f7...e06c

      Index: 4

      scriptSig: 186b...ed3d81 9a9c...0fc5

Input:

      Previous tx: 6b03...e16e

      Index: 7

      scriptSig: c48e...353c81 4afe...2c8d

...

Output:

      Value: 150000000

      scriptPubKey: 2 67c1...4a70 bf9a...f9e3 cffd...1373 3
      OP_CHECKMULTISIG

...
```

8. The first client signs an inchoate expiration transaction record comprising:

   a. a lock time on or after the expiration timestamp;

   b. an input for receiving the commit amount from a commit transaction;

   c. a first expiration output comprising a first expiration amount and a first condition requiring approval of the first party; and

   d. optionally, a second expiration output comprising a second expiration amount and a condition requiring approval of the second party.

Example inchoate expiration transaction record:

```
Input:

      Previous tx: c215...fc9b

      Index: 0

      scriptSig: OP_0 7d17...0b5101 [sig. placeholder]

...

Output:

      Value: 99995000

      scriptPubKey: OP_DUP OP_HASH160 53a5...8974 OP_EQUALVERIFY
      OP_CHECKSIG

Output:

      Value: 4995000

      scriptPubKey: OP_DUP OP_HASH160 30e6...2511 OP_EQUALVERIFY
      OP_CHECKSIG

...

nLockTime: 2014-06-01T12:34:56Z
```

9. The first client transmits the complete commit transaction record and the inchoate expiration transaction record to the second client who optionally stores the complete commit transaction record in non-transitory memory.

10. The second client creates a complete expiration transaction record by signing the inchoate expiration transaction record and stores the complete expiration transaction record in non-transitory memory.

11. The second client transmits the complete expiration transaction record to the first client.

12. After creating or receiving both the complete commit transaction record and the complete expiration transaction record, the first client submits the first source transaction record to the transfer mechanism to effect the first source transaction.

13. After creating or receiving both the complete commit transaction record and the complete expiration transaction record, the second client submits the second source transaction record to the transfer mechanism to effect the second source transaction.

14. After seeing that both the first source transaction record and second source transaction record have been submitted, one or both of the first client the second client submits the complete commit transaction record to the transfer mechanism to effect the commit transaction.

15. At a time or upon an event as defined by the terms or upon a query by the first client or the second client (optionally providing one or more of the complete commit transaction record, a reference to the commit transaction, and the terms), and before the lock time of the complete expiration transaction record, the facilitator performs a calculation in accordance with the terms for determining a first disbursement amount, and optionally a second disbursement amount, optionally requesting information from the data source for use in the calculation (e.g., whether an anticipated shipment has been delivered to a shipper, a destination address, etc., etc.). This could be via an external API, internal database query, etc.

In a typical embodiment, the disbursement amounts are such that any remaining collateral is returned to the respective providing party, and the principal is transferred from the providing party (payer) to the counterparty (payee).

16. The facilitator signs an inchoate disbursement transaction record, which comprises:

a. an input for receiving the commit amount from the commit transaction;

b. a first disbursement output comprising the first disbursement amount and a first condition requiring approval of the second party;

c. optionally, a second disbursement output comprising the second disbursement amount and a condition requiring approval of the first party;

d. optionally a third disbursement output comprising a fee amount and a condition requiring approval of a third party;

typically where the sum of the first disbursement amount, any second disbursement amount, and any fee amount is not more than the commit amount from the commit

transaction.

Example inchoate disbursement transaction record:

```
Input:

      Previous tx: c215...fc9b

      Index: 0

      scriptSig: OP_0 [sig. placeholder] 8205...424901

Output:

      Value: 49990000

      scriptPubKey: OP_DUP OP_HASH160 30e6...2511 OP_EQUALVERIFY
      OP_CHECKSIG

Output:

      Value: 54990000

      scriptPubKey: OP_DUP OP_HASH160 6250...6cfc OP_EQUALVERIFY
      OP_CHECKSIG

Output:

      Value: 10000

      scriptPubKey: OP_DUP OP_HASH160 d377...5c8c OP_EQUALVERIFY
      OP_CHECKSIG

...
```

17. The facilitator transmits the inchoate disbursement transaction record to both the first client and the second client, either of whom can sign and submit it to the transfer mechanism as in the prior example embodiments.

[91] In another embodiment, the condition of the commit output requires approval of either the first party and the second party or the second party and one or more service providers, (e.g., a shipper, insurance provider, inspector, etc.). An inchoate disbursement transaction record is constructed with placeholders for the second party, and each of the service providers. When all

of the service providers have signed their respective portions, the second party may sign and submit the disbursement transaction record to the transfer mechanism. In a further embodiment, the second party commits assets to the commit transaction for paying each of the service providers, and each of the service providers are paid out of the disbursement transaction.

[92] FIGS. 12-14 depict transaction chains from various example L/C embodiments comprising substitutions of parties. FIG. 12 depicts aspects of an embodiment where a payer party (A) has convinced a substituting party (C) to substitute into a transaction with a payee party (B). In addition, the payer party transfers a negotiated amount (ε) to the substituting party. For example, the payer party could have committed to purchasing goods from the payee party, but due to unanticipated market conditions, decided to sell the right to take delivery of the goods to the substituting party at a loss. This is facilitated in the depicted embodiment by a substitution transaction and a second expiration transaction. In a related embodiment where the payer party sold the right to take delivery for a profit, the negotiated amount might flow from the substituting party to the payer party. In the embodiment depicted in FIG. 12, an optional fee (φ) is paid to a third party, and is born by the payee party.

[93] FIG. 13 depicts aspects of an embodiment where a payee party (B) has convinced a substituting party (C) to substitute into a transaction with a payer party (A). In addition, the substituting party transfers a negotiated amount (ε) to the payer party. For example, the third party, may be interested in having the right to receive payment under a future disbursement transaction, perhaps due to the decreasing relative value of the substituting party's other assets. This is facilitated in the depicted embodiment by a substitution transaction, and a second expiration transaction. In a related embodiment where the payee party sold the right to receive payment at a loss, the negotiated amount might flow from the payee party to the substituting party. Similar to FIG. 12, in the embodiment depicted in FIG. 13, an optional fee (φ) is paid to a third party, and is born by the substituting party.

[94] FIG. 14 depicts aspects of an embodiment where a payer party (A) has convinced a substituting party (C) to substitute in part (as depicted to cover the collateral originally paid by the payer party) into a transaction with a payee party (B). In addition, the substituting party transfers a negotiated amount (ε) to the payer party. This is facilitated in the depicted embodiment by a substitution transaction and a second expiration transaction. In some embodiments, the substitution output of the substitute transaction comprises a condition

requiring approval of three of three parties, three of four parties, or two of four parties (e.g., where the substituting party has been delegated authority to approve or sign on behalf of itself and for the payer party). Many possible configurations are contemplated by the invention. In such embodiments, the facilitator can act as a referee in creating the substitution transaction to the satisfaction of all parties, for example, maintaining the ability to dispute the transaction with a chosen mediator as described below.

[95] For clarity of illustration in FIGS. 12-14, the outputs of the commit transaction and the corresponding inputs of the substitution transaction are depicted as separate for each of the first joined principal and collateral ($(P+C)_A$), and the second collateral (C_B). This is not a limitation of the invention. The outputs of the commit transaction, and corresponding inputs of the substitution transaction could be any configuration considered valid by the transfer mechanism. The outputs of the substitution transaction and inputs to the second commit transaction are similarly depicted for clarity of illustration. Again, all valid configurations of inputs and outputs between transactions are contemplated by the invention. Also, in other embodiments, any fee could be paid, in part or in whole, by any party, even a fourth party.

[96] Where a decentralized digital currency (e.g., the Bitcoin protocol, the Ethereum protocol, or similar) is used as the transfer mechanism, another embodiment of the invention enables arbitrary offers—such as offers for arbitrary swaps, L/Cs, and any other offer where terms describing that may be expressed and interpreted by the facilitator—to be made by submitting a specialized transaction record in which the terms, a reference to the terms (e.g., a URI for the terms, a hash of the terms, etc.), or some combination thereof is encoded into the transaction record itself, rather than associated via an extra-transfer mechanism means (i.e., "off block chain" in decentralized digital currency terms), such as a centralized authority, or shared decentralized data store (e.g., a torrent, an "altcoin", etc.).

[97] In one embodiment, this could be encoded as transaction record metadata, or unused data in an input or output (e.g., `<data> OP_DROP <script>`, via the `OP_RETURN <data>` technique in a single output, etc.). For illustration, the following steps describe but a few of many such embodiments:

1. In one embodiment, a first client (offeror) creates an offer transaction record comprising associated data and an offer output comprising an offer amount and a condition requiring approval of one of a first party and, optionally, a facilitator. The associated data comprise one or both of terms and a reference to the terms. Optionally, the associated

data comprise a reference to the facilitator (e.g., a domain name, a payment address, D&B number, URI, etc.). Also optionally, the first client transmits the terms, the associated data, or offer transaction record to the facilitator for validation before submitting it to the transfer mechanism (e.g., to ensure the facilitator can interpret the terms, that the facilitator is appropriately identified, etc.). In another embodiment, at the first client's request, the facilitator creates an inchoate offer transaction record (e.g., not including a signed input) for creating a complete offer transaction record, and the first client optionally verifies whether the facilitator created the inchoate offer transaction record correctly, whether it's available via the facilitator-provided reference (if applicable), etc.

Example inchoate offer transaction record:

```
% # Post the terms to the facilitator
% curl -X POST -d
'{"base":"USD","quote":"AUD","denom":"BTC","pcpl":0.5,"cltl":1.0,"res":
"symunbound","offerexp":"2014-06-01T00:00:00Z","swapexp":"2014-07-
01T00:00:00Z","facuri":"https://facilitator.dom/api/v1"}' ...
https://facilitator.dom/api/v1/swap
{"ok":true,"offersha256":"3a72...f9a4","offerref":"facswap:3a72...f9a4"
,"offeruri":"https://facilitator.dom/api/v1/swap/3a72...f9a4"}

      ID: 9fcd...429c

      ...

      Output:

            Value: 150000000

            scriptPubKey: 666163737761703a3a72...f9a4 OP_DROP 1
            67c1...4a70 cffd...1373 2 OP_CHECKMULTISIG

      ...
```

In this example embodiment, the facilitator prefixes a hash of the terms with "`666163737761703a`", which is hexidecimal for the eight byte ascii string "`facswap:`". This is not necessary, but might be a convenient means by which transactions could be recognized as being of a certain "type", which is useful for monitoring by network

participants.

Alternate embodiment example offer transaction record:

```
% # Post the terms to the facilitator
% curl -X POST -d '{"pubkey":"67c1...4a70","terms":
{"base":"USD",...,"facuri":"https://facilitator.dom/api/v1"}}' ...
https://facilitator.dom/api/v1/swap
{"ok":true,"offersha256":"3a72...f9a4","offerref":"facswap:3a72...f9a4"
,"offeruri":"https://facilitator.dom/api/v1/swap/3a72...f9a4","offertxn
":"04000000...0280d1f008000000008901014b67c1...4a704bcffd...13730102ae.
..00000000000000002a6a28666163737761703a3a72...f9a400000000"}
% # Validate "offertxn", add change outputs, etc.
```

"offertxn" is annotated as follows:

```
04000000 [version: 4] ... 02 [output count: 1] 80d1f00800000000
[amount: 1.5 BTC] 89 [script len: 137] 01 [push next 1 byte] 01 [1] 4b
[push next 75 bytes] 67c1...4a70 [pub. key] 4b [push next 75 bytes]
cffd...1373 [fac. pub. key] 01 [push next 1 byte] 02 [2] ae
[OP_CHECKMULTISIG] ... 0000000000000000 [amount: 0.0 BTC] 2a [script
len: 42] 6a [OP_RETURN] 28 [push next 40 bytes]
666163737761703a3a72...f9a4 [offerref: "facswap:3a72...f9a4"] 00000000
[lock time: none]
```

Note that some parts (such as any inputs or input placeholders) have been skipped with ellipses to assist with readability. In an alternate embodiment, Pay-to-Script Hash (P2SH) is used to obscure the output script that would normally be present in a parent transaction. In such an embodiment the actual output script would be transmitted to the necessary participants via some other means.

2. In one embodiment, the first client creates, or, in another embodiment, the facilitator creates an inchoate commit transaction record for creating a complete commit transaction record much like those described in previous embodiments, except whose first commit input is for accepting the offer amount from the offer transaction, and whose second input is for accepting an amount from a source transaction yet to be identified.

3. The first client creates a complete offer transaction record by signing and the inchoate

offer transaction record and submits it to the transfer mechanism to effect the offer transaction.

4. The facilitator receives the offer transaction from the transfer mechanism.

5. A second client transmits a public key to the facilitator.

6. The facilitator adds the public key to the inchoate commit transaction record and transmits the inchoate commit transaction record to the second client.

7. The second client signs a source transaction record having a transaction ID.

8. The second client adds the transaction ID to the inchoate commit transaction record and signs it.

Example inchoate commit transaction record:

```
Input:
        Previous tx: 9fcd...429c
        Index: 0
        scriptSig: [sig. placeholder]
Input:
        Previous tx: b5e8...6f57
        Index: 6
        scriptSig: 9b6b...8f3701 ac2f...b01b
...
Output:
        Value: 149990000
        scriptPubKey: 2 67c1...4a70 dbe4...4cbe cffd...1373 3
        OP_CHECKMULTISIG
...
```

9. The second client transmits the signed inchoate commit transaction record to the facilitator.

10. Either the first client or, optionally (where allowed), the facilitator creates the complete commit transaction record (e.g., `ID: 6996...ec3d`) by signing the signed inchoate commit transaction record, optionally storing the complete commit transaction record in non-transitory memory.

    Embodiments where one of the first party and the facilitator can approve spending the offer output require the first party to trust the facilitator to perform some verification (e.g., that the source transaction record has sufficient assets, that a nefarious party is not attempting to commit a huge number of very tiny inputs such that the mining fee will be large, or difficult to meet, etc.) and to craft the complete commit transaction record correctly and consistently with the terms.

11. The facilitator creates an inchoate refund or expiration transaction record and transmits the inchoate refund or expiration transaction record to the second client.

12. The second client signs the inchoate refund or expiration transaction record and transmits the signed inchoate refund or expiration transaction record to the facilitator.

13. Either the first client or, optionally (where allowed), the facilitator creates a complete refund or expiration transaction record by signing the inchoate refund transaction record, and stores the complete refund or expiration transaction record in non-transitory memory.

14. The facilitator transmits the complete commit transaction record and the complete refund or expiration transaction record to the second client.

15. The second client submits the source transaction record to the transfer mechanism to effect the source transaction.

16. After seeing that the source transaction has been submitted, one, several, or all of the first client, the second client, and the facilitator submit the complete commit transaction record to the transfer mechanism, after which the process is analogous to previously described embodiments.

[98] In an alternate embodiment, the offer comprises a "hard offer", the condition of the offer

output requires approval of both the first party and the facilitator, and the facilitator signs and transmits to the first party an offer expiration transaction record comprising a lock time set to the time the hard offer expires, an input for receiving the offer amount, and an expiration output comprising an expiration amount and a condition requiring approval of the first party.

[99] In other embodiments of the invention, the transacting parties agree on a third party to act as a mediator in a dispute. For example, if the facilitator becomes unavailable, rather than electing to invoke a refund, one party triggers a dispute whereby a mediator stands in place of the unavailable facilitator. The condition of the commit output of the commit transaction requires approval of two of the first party, the second party, the facilitator, and the mediator. On or after the expiration timestamp, or at a time or upon an event as defined by the terms, and before the lock time of the complete refund transaction record, each of the disputing party and the mediator signs and one party submits a dispute transaction record comprising an input for receiving the commit amount from the commit transaction, and a dispute output comprising a dispute amount and a condition requiring approval of two of the first party, the second party, and the mediator. Once the dispute as been resolved, either the parties sign, or the mediator and one of the parties sign a settlement transaction record similar to the disbursement transaction record above, but reflecting the mediated settlement.

[100] FIGS. 15-16 depict aspects of two such embodiments. In FIG. 15, the dispute transaction further comprises a first fee output comprising a facilitator fee amount (φ_X) and second fee output comprising a mediator fee amount (φ_M), the fees being shared by the parties. In FIG. 16, the dispute transaction comprises the facilitator fee amount shared by the parties, and the settlement transaction comprises the mediator fee amount paid by the party that initiated the dispute (B). In another embodiment, any mediator fee is determined as a term of the settlement, and included with the settlement transaction.

[101] Optionally (and preferably), the parties also sign and transmit to each other a dispute refund transaction record similar to that above, but instead taking its input from the dispute transaction, and with a lock time set in the future with enough time to reach a settlement. This way if the mediator becomes unavailable, the parties can again revert to submitting the dispute refund transaction record. In another embodiment, the dispute transaction could also be "mediatable", allowing for a chain of such disputes, for example naming a second mediator in the event that the mediator becomes unavailable, or the same mediator to allow more time to reach a settlement if the lock time of the dispute refund transaction record is approaching.

[102] In other embodiments, mediation can be automated. For example, in embodiments pertaining to swaps or similar transactions, the facilitator periodically transmits an unsigned disbursement transaction record to the parties as if the trade were halted at the time the unsigned disbursement transaction record is created. The unsigned disbursement transaction comprises a verifiable time at which it was created, or a reference to such a time (e.g., where the transfer mechanism is the Bitcoin or similar protocol, as unused but signed data embedded in one of the scripts, signature by a separate key owned by the facilitator, but not used for signing any inputs, etc.). If the facilitator becomes unavailable before it can transmit to the parties or submit the signed disbursement transaction record, and remains unavailable past the expiration time, a dispute could be initiated, and the parties would have a window during which they have an opportunity to transmit the terms (preferably signed by each party, but this is not necessary if the parties agree on the terms, i.e., both transmit the same terms to the mediator) and some or all of the unsigned disbursement transaction records they received from the facilitator to the mediator. The mediator examines the undisputed or signed terms, and all verifiable unsigned disbursement transaction records received from both parties. In one embodiment, the mediator merely selects the most recent verifiable unsigned disbursement transaction record. In another embodiment, the mediator "plays back" the unsigned disbursement transaction records in order, verifying whether any unsigned disbursement transaction record should have triggered an early exit to the trade (e.g., if principal and any collateral of one party was exhausted). In yet another embodiment, the mediator performs its own independent evaluation of the terms, possibly requesting information from one or more data sources, to stand in place of the facilitator by creating a new settlement transaction record as close to the disbursement transaction record that would have been created by the facilitator if it was available as the mediator is able to determine.

[103] Note that the depicted embodiments are among the more basic of the invention. The various combinations of source transactions, commit transactions, disbursement transactions, refund transactions, expiration transactions, inputs, outputs, and parties, as well as any principal, collateral, or fees, are limited only by the agreements among the participating parties and are enabled by the invention. Additionally, certain steps of the embodiments disclosed throughout this application are described as being performed by certain entities. In other embodiments, similar or equivalent steps could be performed—wholly or partly—by different parties in lieu of or in addition to those described herein. All such embodiments are considered within the scope of the invention.

[104] As a very simple example, in an embodiment using a decentralized digital currency, transactions use P2SH in place of multi-sig transactions. Other steps may be omitted in certain embodiments. For example, in an embodiment using a decentralized digital currency, the creation of the signed complete refund or expiration transaction record—while highly recommended as a contingency to avoid loss in case the facilitator or counterparty disappears or becomes uncooperative—is not strictly necessary to practice the invention. In embodiments involving a mediator, an unsigned dispute transaction record could be created by the facilitator and transmitted to the parties for use with the mediator, for example, at the time the refund or expiration transaction record is created and transmitted.

[105] FIGS. 17-22 depict major phases of effecting a value transfer in the form of a swap within one embodiment using a transfer mechanism comprising a decentralized digital currency comprising a block chain. FIGS. 17-18 depict a first phase, wherein the client validates a first order comprising terms (e.g., base instrument, quote instrument, principal, collateral, disbursement function, expiration timestamp, etc.) with the facilitator. The client submits (broadcasts) a first principal transaction record conforming to the terms to the transfer mechanism to create a first principal transaction. The facilitator monitors the block chain for updates and activates the first order when the first principal transaction has been confirmed. FIG. 19 depicts a second phase, wherein the facilitator matches the first order with a second order, and commits the outputs from the first principal transaction and second principal transaction by creating and submitting (broadcasting) a commit transaction record to the transfer mechanism to create a commit transaction. Optionally, the facilitator also creates and makes available to each client a refund or "rollback" transaction record that spends the outputs from the commit transaction, but cannot be used until well after the expiration timestamp. If the facilitator fails catastrophically, either client can sign and submit the refund transaction record to place both clients back in their original respective positions. FIG. 20 depicts a third phase, where the facilitator receives one or more values from the data source and monitors the valuation by applying the disbursement function to the value(s), the principal, and any collateral to check whether the principal and any collateral of any one party is exhausted. Optionally, each client receives status updates from the facilitator and audits the facilitator's status by independently receiving one or more values from the data source. FIGS. 21-22 depict a final phase, where, after the expiration timestamp (or if the principal and any collateral of any party is exhausted, whichever is sooner), the facilitator creates and signs an inchoate disbursement transaction record that spends the commit transaction's output(s) and comprises one or more disbursement outputs comprising one or more disbursement amounts. Either client receives the

inchoate disbursement transaction record and completes (signs) it to create a completed disbursement transaction record. The client submits (broadcasts) the complete disbursement transaction record to the transfer mechanism to create the disbursement transaction, simultaneously releasing both client's funds.

[106] FIG. 23 depicts the components comprising a typical embodiment of a client (120) or facilitator (100). This comprises a computer processor (160) coupled to a memory (170) and a network interface (190). The computer processor (160) is not limited to a single processing unit as depicted, but could comprise multiple cores, multiple computer processors, a cluster of networked computing devices, or combinations thereof as known in the art. The memory (170) is not limited to a hard disk as depicted, but could comprise any non-transitory memory technology that allows data to be stored in distinct logical sectors (180) (e.g., one or more logical files in a file system, one or more logical records in a file or database, etc.), and that the data persists in the event that the power supply to the computer processor is interrupted. Non-limiting examples include solid state storage, flash drives, RAID, JBOD, NAS, remote storage services such as Amazon's S3 or Google's Cloud Storage, a cluster of memory devices, etc., or combinations as known in the art. In the case of the client (120), the memory (170) comprises one or more logical sectors which comprise one or more key pair sectors for storing an asymmetric key pair (200). In the case of the facilitator (100), the memory (170) comprises one or more logical sectors which comprise one or more key pair sectors (200) as well as one or more transaction record sectors for storing one or more transaction records. The network interface (190) is not limited to a single network interface as depicted. As non-limiting examples, the network interface could comprise multiple network interfaces optionally comprising a load balancer, two or more multiplexed network interfaces, etc., or combinations thereof as known in the art.

[107] FIG. 24 (prior art) depicts a simplified chain of ownership in a decentralized digital currency. In reality, a transaction can have more than one input and more than one output.

INDUSTRIAL APPLICABILITY

[108] The invention pertains to agreements among distinct parties that contemplate transfer of title to property, as well as any industry where that may be of value or importance.

GLOSSARY

[109] These are brief descriptions of terms provided for convenience. They are not intended to

be limiting definitions, but rather to augment any features, characteristics, behaviors, or embodiments that are understood in the art or described elsewhere in the specification.

[110] "client" (120) - A device comprising a computer processor (160), a memory (170) comprising a key pair sector (200) for storing an asymmetric key pair, and a network interface (190), and that is configured to interact with at least one of a facilitator (100) or another client (120, 170) for facilitating value transfers via a transfer mechanism (110) according to the invention.

[111] "cryptocurrency" - See "decentralized digital currency".

[112] "decentralized digital currency" (150) - A transfer mechanism (110) comprising a distributed ledger of transactions (often referred to as a "block chain", e.g., with the Bitcoin protocol and progeny) and typically one or more network participants, the network participants comprising one or more miners. Also referred to as a "cryptocurrency".

[113] "facilitator" (100) - A device for facilitating a value transfer between a first party utilizing a first client (120, 160) and a second party utilizing a second client (120, 170) via a transfer mechanism (110) according to the invention, the device comprising a computer processor (160), a memory (170) comprising a transaction record sector and a key pair sector (200) for storing an asymmetric key pair, and a network interface (190).

[114] "instrument" - A tradable thing of value of any kind; either cash, evidence of an ownership interest in an entity, or a contractual right to receive or deliver cash or another financial instrument. Also referred to as a "financial instrument". According to International Financial Reporting Standards, "any contract that gives rise to a financial asset of one entity and a financial liability or equity instrument of another entity".

[115] "lock time" - A timestamp comprising a date and a time and optionally a time zone that prevents the transaction from being accepted as valid by the transfer mechanism until the timestamp has passed.

[116] "party" - A legal entity capable of exercising property rights, e.g., a person or corporate entity.

[117] "publish[ing] [a] transaction record to [a device]" - Making the transaction record available for reading or copying by the device, for example, by sending the transaction record to the device via a network interface (190), or writing the transaction record to a transaction sector

in a memory in such a way that the transaction record can be read or copied by the device, optionally implementing a permissions scheme allowing the device to read or copy, but not create, update, or destroy the transaction record. Non-limiting examples include a shared file system (e.g., NFS, SSHFS, etc.), a database API (e.g., SQL, REST, etc.), a proprietary API, third party shared storage (e.g., Google Docs, Dropbox, etc.), etc.

[118] "submit[ting] [a] transaction record to [a transfer mechanism (110)]" - The process by which a valid transaction record is accepted by a transfer mechanism (110) to effect a transaction. In the context of a decentralized digital currency (150), this typically comprises broadcasting the transaction record to one or more network participants, having the transaction record accepted by one or more miners who include the transaction record in a valid block that is transmitted to and accepted as valid by a majority of network participants. In the context of decentralized digital currencies (150), acceptance of a transaction as valid by a majority of network participants is permanent and irreversible (except under very limited circumstances, e.g., if the transaction record is later discovered by a majority of network participants to be invalid because it attempted to spend already-spent outputs).

[119] "transaction" - A unit of value transfer in a transfer mechanism (110) that recharacterizes ownership or control of assets (sometimes based on certain conditions). In the context of decentralized digital currencies (150), this is sometimes referred to as a "confirmed transaction", meaning a transaction record that has been accepted into the ledger or block chain by a majority of network participants.

[120] "transaction record" - A data structure describing a transaction and submitted to a transfer mechanism to effect a transaction. As a non-limiting example, in the context of a decentralized digital currency, the transaction record typically comprises one or more inputs (although zero inputs is possible in special cases), one or more outputs, and optionally a cryptographic signature. In the context of decentralized digital currencies (150), this is also (sometimes confusingly) referred to as a "transaction". To avoid ambiguity, this specification uses "transaction record" to refer to the data structure that may be transmitted or received among network participants, and "transaction" to refer to the part of a ledger or block within a block chain comprising the transaction record, the ledger or block being accepted as valid by a majority of network participants (i.e., a "confirmed transaction").

[121] "transfer mechanism" (110) - A means (e.g., a decentralized digital currency) by which a transaction is created (e.g., by successful submission of a transaction record) and enforced.

[122] "value transfer" - The process of transferring a right (e.g., ownership, control, etc.) to one or more items having economic value (e.g., money, goods, services, obligations to perform, etc.) from one party to another.

PTO-1390 (06-13)
Approved for use through 6/30/2013. OMB 0651-0021
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 LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A SUBMISSION UNDER 35 U.S.C. 371

Attorney Docket No.	U.S. Application No. (if known, see 37 CFR 1.5)
2626.P100.US	

International Application No.	International Filing Date	Priority Date Claimed
PCT/US15/29196	05/05/2015	05/09/2014

Title of Invention
Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers

First Named Inventor
Reginald Middleton

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information.

1. [✔] 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 the oath or declaration of the inventor(s) have been received.
2. [ ] A copy of the International Application (35 U.S.C. 371(c)(2)) is attached hereto (not required if the International Application was previously communicated by the International Bureau or was filed in the United States Receiving Office (RO/US)).
3. An English language translation of the International Application (35 U.S.C. 371(c)(2))
   a. [ ] is attached hereto.
   b. [ ] has been previously submitted under 35 U.S.C. 154(d)(4).
4. An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4))
   a. [✔] is attached.
   b. [ ] was previously filed in the international phase under PCT Rule 4.17(iv).

Items 5 to 8 below concern amendments made in the international phase.

PCT Article 19 and 34 amendments

5. [ ] Amendments to the claims under PCT Article 19 are attached (not required if communicated by the International Bureau) (35 U.S.C. 371(c)(3)).
6. [ ] English translation of the PCT Article 19 amendment is attached (35 U.S.C. 371(c)(3)).
7. [ ] English translation of 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

8a. [ ] Do not enter the amendment made in the international phase under PCT Article 19.

8b. [ ] Do not enter the amendment made in the international phase 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).

The following items 9 to 17 concern a document(s) or information included.

9. [ ] An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
10. [ ] A preliminary amendment.
11. [✔] An Application Data Sheet under 37 CFR 1.76.
12. [ ] A substitute specification. NOTE: A substitute specification cannot include claims. See 37 CFR 1.125(b).
13. [✔] A power of attorney and/or change of address letter.
14. [ ] A computer-readable form of the sequence listing in accordance with PCT Rule 13*ter*.3 and 37 CFR 1.821-1.825.
15. [ ] Assignment papers *(cover sheet and document(s))*. Name of Assignee: _____
16. [ ] 37 CFR 3.73(c) Statement *(when there is an Assignee)*.

This collection of information is required by 37 CFR 1.414 and 1.491-1.492. 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 15 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: Mail Stop PCT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

U.S. APPLN. No. (if known – see 37 CFR 1.5)	INTERNATIONAL APPLICATION No.	ATTORNEY DOCKET No.
	PCT/US15/29196	2626.P100.US

17. ☐ Other items or information:

The following fees have been submitted.	CALCULATIONS	PTO USE ONLY
18. ☑ Basic national fee (37 CFR 1.492(a)) **$280**	$ 140	
19. ☑ Examination fee (37 CFR 1.492(c)) If the written opinion prepared by ISA/US or the international preliminary examination report prepared by IPEA/US indicates all claims satisfy provisions of PCT Article 33(1)-(4) ..... **$0** All other situations **$720**	360 $	
20. ☑ Search fee (37 CFR 1.492(b)) If the written opinion prepared by ISA/US or the international preliminary examination report prepared by IPEA/US indicates all claims satisfy provisions of PCT Article 33(1)-(4) ..... **$0** Search fee (37 CFR 1.445(a)(2)) has been paid on the international application to the USPTO as an International Searching Authority ..... **$120** International Search Report prepared by an ISA other than the US and provided to the Office or previously communicated to the US by the IB ..... **$480** All other situations **$600**	60 $	
TOTAL OF 18, 19, and 20 =	$560	
☐ Additional fee for specification and drawings filed in paper over 100 sheets (excluding sequence listing in compliance with 37 CFR 1.821(c) or (e) in an electronic medium or computer program listing in an electronic medium) (37 CFR 1.492(j)). Fee for each additional 50 sheets of paper or fraction thereof **$400**		

Total Sheets	Extra Sheets	Number of each addition 50 or fraction thereof (round up to a whole number)	RATE	
- 100 =	/ 50 =		x $400	$

Surcharge of **$140.00** for furnishing any of the search fee, examination fee, or the oath or declaration after the date of commencement of the national stage (37 CFR 1.492(h)).	$	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	30 - 20 =	10	x $80	$400	
Independent claims	3 - 3 =	0	x $420	$0	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ $780	$	
Processing fee of **$140.00** for furnishing the English translation later than 30 months from the earliest claimed priority date (37 CFR 1.492(i)). +				$	
TOTAL OF ABOVE CALCULATIONS =				$	
☑ **Applicant asserts small entity status.** See 37 CFR 1.27. Fees above are reduced by ½.					
☐ **Applicant certifies micro entity status.** See 37 CFR 1.29. Fees above are reduced by ¾. Applicant must attach form PTO/SB/15A or B or equivalent.					
TOTAL NATIONAL FEE =				$960	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property. +				$	
TOTAL FEES ENCLOSED =				$960	
				Amount to be refunded:	$
				Amount to be charged:	$

a. ☐ A check in the amount of $_____ to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. _____ in the amount of $_____ to cover the above fees.

c. ☐ The Director is hereby authorized to charge additional fees which may be required, or credit any overpayment, to Deposit Account No. _____ as follows:

i. ☐ any required fee.

ii. ☐ any required fee except for excess claims fees required under 37 CFR 1.492(d) and (e) and multiple dependent claim fee required under 37 CFR 1.492(f).

d. ☑ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038. The PTO-2038 should only be mailed or faxed to the USPTO. However, when paying the basic national fee, the PTO-2038 may NOT be faxed to the USPTO.

ADVISORY: If filing by EFS-Web, do **NOT** attach the PTO-2038 form as a PDF along with your EFS-Web submission. Please be advised that this is **not** recommended and by doing so your **credit card information may be displayed via PAIR**. To protect your information, it is recommended to pay fees online by using the electronic payment method.

NOTE: Where an appropriate time limit under 37 CFR 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the International Application to pending status.

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 1: 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.**

NOTE 2: 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

☑ The address associated with Customer Number: 11238 **OR** ☐ Correspondence address below

Name					
Address					
City		State		Zip Code	
Country		Telephone			
Email					

Signature	/JohnNielsen53392/	Date	11/4/2016
Name (Print/Type)	John Nielsen	Registration No. (Attorney/Agent)	53,392

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers
First Named Inventor/Applicant Name:	Reginald Middleton
Filer:	John Nielsen
Attorney Docket Number:	2626.P100.US

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	140	140
Natl Stage Search Fee - U.S. was the ISA	2641	1	60	60
NATL STAGE EXAM FEE - ALL OTHER CASES	2633	1	360	360
Pages:				
Claims:				
CLAIMS IN EXCESS OF 20	2615	10	40	400
Miscellaneous-Filing:				
Petition:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**960**

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
15/309,612	11/08/2016		960	2626.P100.US	30	3

CONFIRMATION NO. 2321

115238
Sentinel IP
484 Washington Street
Suite B345
Monterey, CA 93940

FILING RECEIPT

OC000000090039580

Date Mailed: 03/22/2017

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)

Reginald Middleton, Brooklyn, NY;
Matthew Bogosian, Anacortes, WA;

Applicant(s)

Veritaseum, Inc., Brooklyn, NY;
Reginald Middleton, Brooklyn, NY
Matthew Bogosian, Anacortes, WA

Power of Attorney: The patent practitioners associated with Customer Number 115238

Domestic Priority data as claimed by applicant

This application is a 371 of PCT/US15/29196 05/05/2015
which claims benefit of 61/990,795 05/09/2014

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

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: 03/20/2017

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 15/309,612**

Projected Publication Date: 06/29/2017

Non-Publication Request: No

Early Publication Request: No
**** SMALL ENTITY ****
Title

Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers

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.

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.
15/309,612	Reginald Middleton	2626.P100.US

115238
Sentinel IP
484 Washington Street
Suite B345
Monterey, CA 93940

INTERNATIONAL APPLICATION NO.	
PCT/US2015/029196	
I.A. FILING DATE	PRIORITY DATE
05/05/2015	05/09/2014

CONFIRMATION NO. 2321
371 ACCEPTANCE LETTER

OC000000090039561

Date Mailed: 03/22/2017

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)

11/08/2016
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 11/08/2016
- Copy of the International Search Report filed on 11/08/2016
- Inventor's Oath or Declaration filed on 11/08/2016
- Request for Immediate Examination filed on 11/08/2016
- U.S. Basic National Fees filed on 11/08/2016
- Authorize Access to Search Results filed on 11/08/2016
- Priority Documents filed on 11/08/2016
- Power of Attorney filed on 11/08/2016
- Authorization to Permit Access filed on 11/08/2016
- Application Data Sheet (37 CFR 1.76) filed on 11/08/2016

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)

JACQUELINE A WHITFIELD

Telephone: (703) 756-1132

MULTIPLE DEPENDENT CLAIM FEE CALCULATION SHEET

Substitute for Form PTO-1360
(For use with Form PTO/SB/06)

Application Number	Filing Date
15309612	

Applicant(s) Reginald Middleton

* 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		1				
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						
32						
33						
34						
35						
36						
37						
38						
39						
40						
41						
42						
43						
44						
45						
46						
47						
48						
49						
50						
Total Indep	3		0		0	
Total Depend	27	↵	0	↵	0	↵
Total Claims	30		0		0	

	*		*		*	
	Indep	Depend	Indep	Depend	Indep	Depend
51						
52						
53						
54						
55						
56						
57						
58						
59						
60						
61						
62						
63						
64						
65						
66						
67						
68						
69						
70						
71						
72						
73						
74						
75						
76						
77						
78						
79						
80						
81						
82						
83						
84						
85						
86						
87						
88						
89						
90						
91						
92						
93						
94						
95						
96						
97						
98						
99						
100						

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 15/309,612

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	140		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	300		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	360		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	30 minus 20 =	* 10	x 40 =	400	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*	x 210 =	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).			0.00			
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	1200		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.

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
15/309,612	11/08/2016	Reginald Middleton	2626.P100.US

CONFIRMATION NO. 2321

115238
Sentinel IP
484 Washington Street
Suite B345
Monterey, CA 93940

PUBLICATION NOTICE

OC000000092444356

Title: Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers

Publication No.US-2017-0187535-A1
Publication Date:06/29/2017

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

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. 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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	15309612
Filing Date	2016-08-11
First Named Inventor	Middleton; Reginald
Art Unit	3685
Examiner Name	HEWITT II, CALVIN L
Attorney Docket Number	

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20030070080	A1	2003-04-10	Sholom S. Rosen	
	2	20130166455	A1	2013-06-27	Feigelson Douglas	
	3	20130212388	A1	2013-08-15	Peter et. al.	
	4	20130054471	A1	2013-02-28	Samid Gideon	
	5	20130179337	A1	2013-07-11	Ochynski Walter	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15309612
	Filing Date	2016-08-11
	First Named Inventor	Middleton; Reginald
	Art Unit	3685
	Examiner Name	HEWITT II, CALVIN L
	Attorney Docket Number	

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15309612
	Filing Date	2016-08-11
	First Named Inventor	Middleton; Reginald
	Art Unit	3685
	Examiner Name	HEWITT II, CALVIN L
	Attorney Docket Number	

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Vani Moodley/	Date (YYYY-MM-DD)	2018-03-01
Name/Print	Vani Moodley	Registration Number	56631

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1 hour 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.**

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 record s.

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 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.

Electronic Acknowledgement Receipt

EFS ID:	31927128
Application Number:	15309612
International Application Number:	
Confirmation Number:	2321
Title of Invention:	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers
First Named Inventor/Applicant Name:	Reginald Middleton
Customer Number:	115238
Filer:	Vani Moodley/Ashutosh choudhary
Filer Authorized By:	Vani Moodley
Attorney Docket Number:	2626.P100.US
Receipt Date:	01-MAR-2018
Filing Date:	08-NOV-2016
Time Stamp:	04:30:25
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	D360USPCT_POA_Executed.pdf	467246 075ac2eb7753b7838fede7a8921ac342d2c57d2c	no	1

Warnings:

Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	IDS1.pdf	612178 2338dfc3b46ce3b4552fecb1dcb02b674146489f	no	4
Warnings:					
Information:					
3	Other Reference-Patent/App/Search documents	US2003070080A1.pdf	16729632 1f095454e42333bf7b9ec7143458a1a5f42b7aa6	no	271
Warnings:					
Information:					
4	Other Reference-Patent/App/Search documents	US2013054471A1.pdf	3494687 b90bc9364fd4538b057d4ebfb1fdf430bf30940b	no	35
Warnings:					
Information:					
5	Other Reference-Patent/App/Search documents	US2013166455A1.pdf	1265790 3cb6c0464a620a54363457147f42f9dbd0d15f3b	no	22
Warnings:					
Information:					
6	Other Reference-Patent/App/Search documents	US2013179337A1.pdf	1084025 f59e1042c940558b9182ab504d5759bd9b10df56	no	14
Warnings:					
Information:					
7	Other Reference-Patent/App/Search documents	US2013212388A1.pdf	3216714 febe5bd5e22a6f6f2eac5c1741b5c3d89c3e1db5	no	27
Warnings:					
Information:					
			Total Files Size (in bytes):	26870272	

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.

Doc Code: PA.
Document Description: Power of Attorney

PTO/AIA/82B (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
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
15309612	11/08/2016

(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: 52418

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):

Veritaseum, Inc.

☐ 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	Eleanor R. Reid	Date (Optional)	
Name	Reid, Eleanor		
Title	Vice President, Operations, Veritaseum, Inc.		

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.

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
15/309,612	11/08/2016	Reginald Middleton	2626.P100.US

CONFIRMATION NO. 2321

POWER OF ATTORNEY NOTICE

115238
Sentinel IP
484 Washington Street
Suite B345
Monterey, CA 93940

OC000000097789084

Date Mailed: 03/06/2018

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 03/01/2018.

- The Power of Attorney to you in this application has been revoked by the applicant. Future correspondence will be mailed to the new address of record(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**.

/ttran/

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
15/309,612	11/08/2016	Reginald Middleton	2626.P100.US

CONFIRMATION NO. 2321

52418
HM Law Group LLP
19925 Stevens Creek Blvd.
Suite 100
Cupertino, CA 95014-2358

POA ACCEPTANCE LETTER

OC000000097789196

Date Mailed: 03/06/2018

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 03/01/2018.

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**.

/ttran/

Electronic Acknowledgement Receipt

EFS ID:	35894713
Application Number:	15309612
International Application Number:	
Confirmation Number:	2321
Title of Invention:	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers
First Named Inventor/Applicant Name:	Reginald Middleton
Customer Number:	52418
Filer:	Carl Irwin Brundidge
Filer Authorized By:	
Attorney Docket Number:	D360USPCT
Receipt Date:	01-MAY-2019
Filing Date:	08-NOV-2016
Time Stamp:	20:53:36
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	2019-04-10-VeritaseumINC-Patent-Genl-POA.pdf	1190068 381b1f275777d7b979b87cb77f38ca9f8980ff4d	no	1

Warnings:

Information:	
Total Files Size (in bytes):	1190068

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.

PTO/AIA/80 (07-17)
Approved for use through 05/31/2021. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no person is required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(c).

I hereby appoint:

[X] Practitioners associated with Customer Number: 86636

OR

[ ] Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number

Name	Registration Number

As attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(c).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(c) to:

[X] The address associated with Customer Number: 86636

OR

[ ]

Firm or individual name		
Address		
City	State	Zip
Country		
Telephone	Email	

Assignee name and address: Veritaseum, Inc., 195 Argyle Road, Brooklyn NY 11218

A copy of this form, together with a statement under 37 CFR 3.73(c) (Form PTO/AIA/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(c) may be completed by one of the practitioners appointed in this form, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee.

Signature [signature]	Date 4/10/19
Name Reggie Middleton	Telephone 718-407-4751
Title CEO	

This collection of information is required by 37 CFR 1.31, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public, which is to update (and by the USPTO to process) the file of a patent or reexamination proceeding. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 18 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.

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
15/309,612	11/08/2016	Reginald Middleton	D360USPCT

CONFIRMATION NO. 2321

POWER OF ATTORNEY NOTICE

52418
HM Law Group LLP
19925 Stevens Creek Blvd.
Suite 100
Cupertino, CA 95014-2358

OC000000107904026

Date Mailed: 05/03/2019

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 05/01/2019.

- The Power of Attorney to you in this application has been revoked by the applicant. Future correspondence will be mailed to the new address of record(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**.

/mbeyene/

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
15/309,612	11/08/2016	Reginald Middleton	D360USPCT

CONFIRMATION NO. 2321

86636
BRUNDIDGE & STANGER, P.C.
1925 BALLENGER AVENUE, STE. 560
ALEXANDRIA, VA 22314

POA ACCEPTANCE LETTER

OC000000107904054

Date Mailed: 05/03/2019

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 05/01/2019.

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**.

/mbeyene/

Notice of References Cited	Application/Control No. 15/309,612	Applicant(s)/Patent Under Reexamination Middleton et al.	
	Examiner JAMES D NIGH	Art Unit 3685	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-20130166455-A1	06-2013	Feigelson; Douglas	H04L9/3234	705/64
*	B	US-20030070080-A1	04-2003	Rosen, Sholom S.	G06Q20/02	713/187
	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	
	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.

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. 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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	15309612
Filing Date	2016-08-11
First Named Inventor	Middleton; Reginald
Art Unit	3685
Examiner Name	HEWITT II, CALVIN L
Attorney Docket Number	

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20030070080	A1	2003-04-10	Sholom S. Rosen	
	2	20130166455	A1	2013-06-27	Feigelson Douglas	
	3	20130212388	A1	2013-08-15	Peter et. al.	
	4	20130054471	A1	2013-02-28	Samid Gideon	
	5	20130179337	A1	2013-07-11	Ochynski Walter	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.D.N/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	15309612
Filing Date	2016-08-11
First Named Inventor	Middleton; Reginald
Art Unit	3685
Examiner Name	HEWITT II, CALVIN L
Attorney Docket Number	

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/JAMES D NIGH/	Date Considered	07/20/2019

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.D.N/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	15309612
Filing Date	2016-08-11
First Named Inventor	Middleton; Reginald
Art Unit	3685
Examiner Name	HEWITT II, CALVIN L
Attorney Docket Number	

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Vani Moodley/	Date (YYYY-MM-DD)	2018-03-01
Name/Print	Vani Moodley	Registration Number	56631

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1 hour 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.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.D.N/

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 record s.

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 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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.D.N/

Bibliographic Data

Application No: 15/309,612

Foreign Priority claimed: ○ Yes ◉ No

35 USC 119 (a-d) conditions met: ☐ Yes ☑ No ☐ Met After Allowance

Verified and Acknowledged: /JAMES D NIGH/ Examiner's Signature | Initials

Title: Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers

---

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
11/08/2016	705	3685	4675.1002BS
RULE			

APPLICANTS

Veritaseum, Inc., Brooklyn, NY, UNITED STATES

INVENTORS

Reginald Middleton Brooklyn, NY, UNITED STATES

Matthew Bogosian Anacortes, WA, UNITED STATES

CONTINUING DATA

This application is a 371 of PCT/US15/29196 05/05/2015

PCT/US15/29196 has PRO of 61990795 05/09/2014

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

03/20/2017

**** SMALL ENTITY ****

STATE OR COUNTRY

UNITED STATES

ADDRESS

BRUNDIDGE & STANGER, P.C.
1925 BALLENGER AVENUE, STE. 560
ALEXANDRIA, VA 22314
UNITED STATES

FILING FEE RECEIVED

$960

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.
15/309,612	11/08/2016	Reginald Middleton	4675.1002BS	2321

86636 7590 07/24/2019

BRUNDIDGE & STANGER, P.C.
1925 BALLENGER AVENUE, STE. 560
ALEXANDRIA, VA 22314

EXAMINER	
NIGH, JAMES D	

ART UNIT	PAPER NUMBER
3685	

MAIL DATE	DELIVERY MODE
07/24/2019	PAPER

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.

Office Action Summary	Application No. 15/309,612	Applicant(s) Middleton et al.	
	Examiner JAMES D NIGH	Art Unit 3685	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 08 November 2016.

☐ 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) 1-30 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) 1-30 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 08 November 2016 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 03/01/2018.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

DETAILED ACTION

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. Applicant's claim for the benefit of U.S. provisional patent application 61/990,795 filed May 9, 2014 under 35 U.S.C. 119(e) is acknowledged.

Information Disclosure Statement

3. The information disclosure statement (IDS) was submitted on March 1, 2018. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Rejections - 35 USC § 112

4. 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.

5. Claims 13, 27 and 30 are 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.

6. Claim 13 recites "where: a. the first computer processor consists of the second computer processor; b. the first memory consists of the second memory; and c. the first network interface consists of the second network interface". Claims 27 and 30 contain

similar recitations. It is unclear how one processor or memory can "consist of" another processor or memory and still be considered as separate structure, particularly when they have been assigned to separate pieces of structure "An essential purpose of patent examination is to fashion claims that are precise, clear, correct, and unambiguous. Only in this way can uncertainties of claim scope be removed…", In re Zletz,13 USPQ2d 1320 (Fed. Cir. 1989)

7. The following is a quotation of 35 U.S.C. 112(d):

> (d) REFERENCE IN DEPENDENT FORMS.—Subject to subsection (e), a claim in dependent form shall contain a reference to a claim previously set forth and then specify a further limitation of the subject matter claimed. A claim in dependent form shall be construed to incorporate by reference all the limitations of the claim to which it refers.

The following is a quotation of pre-AIA 35 U.S.C. 112, fourth paragraph:

> Subject to the following paragraph [i.e., the fifth paragraph of pre-AIA 35 U.S.C. 112], a claim in dependent form shall contain a reference to a claim previously set forth and then specify a further limitation of the subject matter claimed. A claim in dependent form shall be construed to incorporate by reference all the limitations of the claim to which it refers.

8. Claims 13, 27 and 30 are rejected under 35 U.S.C. 112(d) or pre-AIA 35 U.S.C. 112, 4th paragraph, as being of improper dependent form for failing to further limit the subject matter of the claim upon which it depends, or for failing to include all the limitations of the claim upon which it depends.

9. Claim 13 recites "where: a. the first computer processor consists of the second computer processor; b. the first memory consists of the second memory; and c. the first network interface consists of the second network interface". Claims 27 and 30 contain similar recitations. As these were claimed as separate units of structure in claim 12 by saying that the "first…consists of the second" the claim is removing a limitation of claim 12 and thus is rejected under paragraph d of section 112. Similar reasoning applies to claims 27 and 30.

10. Applicant may cancel the claim(s), amend the claim(s) to place the claim(s) in proper dependent form, rewrite the claim(s) in independent form, or present a sufficient showing that the dependent claim(s) complies with the statutory requirements.

Claim Rejections - 35 USC § 102

11. 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.

12. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a)(1) the claimed invention was patented, described in a printed publication, or in public use, on sale or otherwise available to the public before the effective filing date of the claimed invention.
>
> (a)(2) the claimed invention was described in a patent issued under section 151, or in an application for patent published or deemed published under section 122(b), in which the patent or application, as the case may be, names another inventor and was effectively filed before the effective filing date of the claimed invention.

13. Claims 1 and 3-11 are rejected under 35 U.S.C. 102(a)(1) and (a)(2) as being anticipated by Rosen (U.S. Patent Publication 2003/0070080).

14. As per claim 1

Rosen discloses a device for facilitating a value transfer between a first party utilizing a first client and a second party utilizing a second client via a transfer mechanism (0026, 0149-0151, 0161 “The Pay/Exchange application 35 supervises the

sending and receiving of electronic notes 11 between Transaction money modules 4", Figure 56)

Rosen discloses a first memory comprising a transaction record sector and a first key pair sector for storing a first asymmetric key pair, the first asymmetric key pair comprising a first private key and a first public key (0162 "The Tran Log Mgr. application 36 provides the management and overseeing of a log that records completed transactions undertaken by the money module", 0685-0688 "Each primary trusted server 210 has its own public key and corresponding private key", claim 1, claim 2, claim 13)

Rosen discloses a first network interface for receiving terms (0231-0234)

Rosen discloses the terms comprising a first principal amount (0165)

Rosen discloses a reference to a first data source (0159, 1297)

Rosen discloses a first computer processor coupled to the first memory and the first network interface, the first computer processor configured to: retrieve a value from the first data source (0149, 0677)

Rosen discloses read the first private key from the first key pair sector (0504, claim 13)

Rosen discloses compute a first cryptographic signature from the first private key (0660, 0662, 0702)

Rosen discloses create an inchoate disbursement transaction record comprising: a commit input for receiving a commit amount from a commit transaction (0157, 0546, 1941)

Rosen discloses the first cryptographic signature (1946)

Rosen discloses publish the inchoate disbursement transaction record to at least one of the first client and the second client (0142-0143, 0588-0591, Figure 3, Figure 7, Figure 36A)

Rosen discloses where the first client comprises: a second memory comprising a second key pair sector for storing a second asymmetric key pair, the second asymmetric key pair comprising a second private key and a second public key (0142-0143, 0159, 0191, 0662, 0749, claim 91)

Rosen discloses a second network interface (0666)

Rosen discloses a second computer processor coupled to the second memory and the second network interface, the second computer processor configured to read the second private key from the second key pair sector (0630, 0664, 0749, Figure 52)

Rosen discloses where the second client comprises a third memory comprising a third key pair sector for storing a third asymmetric key pair, the third asymmetric key pair comprising a third private key and a third public key (1660-1663, Figure 57A)

Rosen discloses a third network interface (0670)

Rosen discloses a third computer processor coupled to the third memory and the third network interface, the third computer processor configured to read the third private key from the third key pair sector (0664, 1660-1663, Figure 56)

15. As per claim 3

Rosen discloses where: the first computer processor is further configured to compute a disbursement amount by applying a disbursement function to: the first principal amount; and the value from the first data source: and the inchoate

disbursement transaction record further comprises a disbursement output comprising the disbursement amount (0157-0174)

16. As per claim 4

Rosen discloses where the first computer processor is further configured to: a. compute a second cryptographic signature from the first private key; b. create an inchoate refund transaction record comprising: . a commit input for receiving the commit amount from the commit transaction: ii. a refund output comprising a refund amount; iii. the second cryptographic signature; and iv. a lock time; and c. publish the inchoate refund transaction record to at least one of the first client or the second client (0157-0174, 0176-0179, 0251, 0300, 0806-0807, 0845)

17. As per claim 5

Rosen discloses where: a. the first key pair sector further stores a fourth asymmetric key pair, the fourth asymmetric key pair comprising a fourth private key and a fourth public key; and b. the first computer processor is further configured to: i. read the fourth private key from the first key pair sector; ii. compute a second cryptographic signature from the fourth private key; iii. create a commit transaction record, the commit transaction record comprising: A. a first principal input for receiving the first principal amount from a first principal transaction; B. a commit output comprising the commit amount; C. the second cryptographic signature; and iv. create the commit transaction by submitting the commit transaction record to the transfer mechanism (0177, 0193, 0546, 0662, 0791-0802, claims 1, 2 and 13)

18. As per claim 6

Rosen discloses where the first asymmetric key pair consists of the fourth asymmetric key pair, the first private key consists of the fourth private key, and the first public key consists of the fourth public key (0193, 0683-0688, 0854, Figure 56, claim 13)

19. As per claim 7

Rosen discloses where: a. the terms further comprise: i. a second principal amount; and ii. an expiration timestamp; b. the first computer processor is further configured to compute the one or more disbursement amounts by applying a disbursement function to: i. the value from the first data source; and at least one of: A. the first principal amount; and B. the second principal amount; and c. the inchoate disbursement transaction record further comprises one or more disbursement outputs comprising the disbursement amounts (0157-0174, 0176-0179, 0184, 0535, 0798-0802).

20. As per claim 8

Rosen discloses where: a, the terms further comprise: i, a reference to a second data source; b. the first computer processor is further configured to compute the one or more disbursement amounts by applying the disbursement function to: L. the value from the first data source; ii. the value from the second data source; iii. the first principal amount; and iv. the second principal amount (0157-0174, 0176-0179, 0184, 0279, 0284).

21. As per claim 9

Rosen discloses where: a. the reference to the first data source comprises at least one of a reference to a base instrument and a reference to a quote instrument;

and b. the first computer processor is further configured to compute the disbursement amounts on or after the expiration timestamp (0118, 0180, 0278, 0284, 0535-0540, 0628)

22. As per claim 10

Rosen discloses where the first computer processor is further configured to: a. compute a second cryptographic signature from the first private key; b. create an inchoate refund transaction record comprising: L. a commit input for receiving the commit amount from the commit transaction; ii. one or more refund outputs comprising one or more refund amounts; iii. the second cryptographic signature; and iv. a lock time; and c. publish the inchoate refund transaction record to at least one of the first client and the second client (0157-0174, 0176-0179, 0251, 0300, 0806-0807, 0845)

23. As per claim 11

Rosen discloses where: a. the first key pair sector further stores a fourth asymmetric key pair, the fourth asymmetric key pair comprising a fourth private key and a fourth public key; and b. the first computer processor is further configured to: i. read the fourth private key from the first key pair sector; ii. compute a second cryptographic signature from the fourth private key; iii. create a commit transaction record comprising: A. a first principal input for receiving the first principal amount from a first principal transaction; B. a second principal input for receiving the second principal amount from a second principal transaction; C. a commit output comprising a commit amount; and D. the second cryptographic signature; and iv. create the commit transaction by submitting the commit transaction record to the transfer mechanism (0177, 0193, 0255-0267, 0546, 0662, 0791-0802, 1723, claims 1, 2 and 13).

Claim Rejections - 35 USC § 103

24. 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.

25. Claims 12-30 are rejected under 35 U.S.C. 103 as being unpatentable over Rosen in view of Feigelson.

26. As per claim 2

Rosen, while disclosing electronic money (Abstract), does not explicitly disclose wherein the transfer mechanism comprises a decentralized currency. Feigelson teaches wherein the transfer mechanism comprises a decentralized currency (0050-0051)

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the electronic monetary system of Rosen with the creation and use of digital currency of Feigelson for the purpose of maintaining secrecy of information in order to control its value (0003).

27. Claims 12-30 are rejected under 35 U.S.C. 103 as being unpatentable over Rosen as applied to claim 1 above, and further in view of Feigelson (U.S. Patent Publication 2013/0166455).

28. As per claim 12

Rosen discloses a device for facilitating a value transfer between a first party utilizing a first client and a second party utilizing a second client via a transfer

mechanism (0026, 0149-0151, 0161 “The Pay/Exchange application 35 supervises the sending and receiving of electronic notes 11 between Transaction money modules 4”, Figure 56)

Rosen discloses a first memory comprising a transaction record sector and a first key pair sector for storing a first asymmetric key pair, the first asymmetric key pair comprising a first private key and a first public key (0162 “The Tran Log Mgr. application 36 provides the management and overseeing of a log that records completed transactions undertaken by the money module”, 0685-0688 “Each primary trusted server 210 has its own public key and corresponding private key”, claim 1, claim 2, claim 13)

Rosen discloses a first network interface for receiving terms (0231-0234)

Rosen discloses the terms comprising a first principal amount (0165)

Rosen discloses a reference to a first data source (0159, 1297)

Rosen discloses a first computer processor coupled to the first memory and the first network interface, the first computer processor configured to: retrieve a value from the first data source (0149, 0677)

Rosen discloses read the first private key from the first key pair sector (0504, claim 13)

Rosen discloses compute a first cryptographic signature from the first private key (0660, 0662, 0702)

Rosen discloses create an inchoate disbursement transaction record comprising: a commit input for receiving a commit amount from a commit transaction (0157, 0546, 1941)

Rosen discloses the first cryptographic signature (1946)

Rosen discloses publish the inchoate disbursement transaction record to at least one of the first client and the second client (0142-0143, 0588-0591, Figure 3, Figure 7, Figure 36A)

Rosen discloses where the first client comprises: a second memory comprising a second key pair sector for storing a second asymmetric key pair, the second asymmetric key pair comprising a second private key and a second public key (0142-0143, 0159, 0191, 0662, 0749, claim 91)

Rosen discloses a second network interface (0666)

Rosen discloses a second computer processor coupled to the second memory and the second network interface, the second computer processor configured to read the second private key from the second key pair sector (0630, 0664, 0749, Figure 52)

Rosen discloses where the second client comprises a third memory comprising a third key pair sector for storing a third asymmetric key pair, the third asymmetric key pair comprising a third private key and a third public key (1660-1663, Figure 57A)

Rosen discloses a third network interface (0670)

Rosen discloses a third computer processor coupled to the third memory and the third network interface, the third computer processor configured to read the third private key from the third key pair sector (0664, 1660-1663, Figure 56)

Rosen, while disclosing electronic money (Abstract), does not explicitly disclose wherein the transfer mechanism comprises a decentralized currency. Feigelson teaches wherein the transfer mechanism comprises a decentralized currency (0050-0051)

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the electronic monetary system of Rosen with the creation and use of digital currency of Feigelson for the purpose of maintaining secrecy of information in order to control its value (0003).

29. As per claim 13

Rosen discloses where: a. the first computer processor consists of the second computer processor; b. the first memory consists of the second memory; and c. the first network interface consists of the second network interface (0143, 0147, 0157)

30. As per claims 14 and 25

Rosen discloses where: the first computer processor is further configured to compute a disbursement amount by applying a disbursement function to: the first principal amount; and the value from the first data source: and the inchoate disbursement transaction record further comprises a disbursement output comprising the disbursement amount (0157-0174, 0177, 0193, 0288, 0504, 0546, 0662, 0791-0802, claims 1, 2 and 13)

31. As per claim 15

Rosen discloses where the first computer processor is further configured to: a. compute a second cryptographic signature from the first private key; b. create an inchoate refund transaction record comprising: i. a commit input for receiving the commit amount from the commit transaction; ii. a refund output comprising a refund amount; and iii. the second cryptographic signature; and c. publish the inchoate refund transaction record to at least one of the first client and the second client. (0176-0179, 0251, 0300, 0806-0807)

32. As per claim 16

Rosen discloses where: a. the first key pair sector further stores a fourth asymmetric key pair, the fourth asymmetric key pair comprising a fourth private key and a fourth public key; b. the first computer processor is further configured to: i. compute a disbursement amount by applying a disbursement function to: A. the first principal amount; and B. the value from the first data source; ii. read the fourth private key from the first key pair sector; iii. compute a second cryptographic signature from the fourth private key; iv. create a commit transaction record comprising: A. a first principal input for receiving the first principal amount from a first principal transaction; B. a commit output comprising the commit amount; and C. the second cryptographic signature; and v. create the commit transaction by submitting the commit transaction record to the transfer mechanism; and c. the inchoate disbursement transaction record further comprises a disbursement output comprising the disbursement amount (0157-0174, 0177, 0193, 0546, 0662, 0791-0802, claims 1, 2 and 13)

33. As per claim 17

Rosen discloses where the second computer processor is configured to: a. compute a third cryptographic signature from the second private key; b. create a first principal transaction record comprising: i. a first principal output comprising the first principal amount; and ii. the third cryptographic signature; and c. create the first principal transaction by submitting the first principal transaction record to the transfer mechanism (0157-0174, 0176-0179, 0300, 0791-0802)

34. As per claim 18

Rosen discloses where: a. the terms further comprise: i. a second principal amount; and ii. an expiration timestamp; b. the first computer processor is further configured compute one or more disbursement amounts by applying a disbursement function to: i, the value from the first data source; and at least one of: A. the first principal amount; and B. the second principal amount; c. the inchoate disbursement transaction record further comprises one or more disbursement outputs comprising the disbursement amounts; and d. the second computer processor is further configured to: i. read the inchoate disbursement transaction; ii. compute a second cryptographic signature from the second private key; iii. create a complete disbursement transaction record comprising :A. the commit input; B. the disbursement outputs; C. the first cryptographic signature; and D. the second cryptographic signature; and iv. create a disbursement transaction by submitting the complete disbursement transaction record to the transfer mechanism (0157-0174, 0176-0179, 0288, 0504, 0535, 0546, 0791-0802)

35. As per claim 19

Rosen discloses where: a. the terms further comprise: i. a reference to a second data source; b. the first computer processor is further configured to compute the one or more disbursement amounts by applying the disbursement function to: i, the value from the first data source; i. the value from the second data source; iii. the first principal amount; and iv. the second principal amount (0157-0174, 0176-0179, 0184, 0279, 0284)

36. As per claim 20

Rosen discloses where: a. the reference to the first data source comprises at least one of a reference to a base instrument and a reference to a quote instrument; and b. the first computer processor is further configured to compute the disbursement amounts on or after the expiration timestamp (0118, 0180, 0278, 0284, 0535-0540, 0628)

37. As per claim 21

Rosen discloses where: a. the terms further comprise: i. a second principal amount; and ii. an expiration timestamp; b. the first computer processor is further configured to: i. compute one or more disbursement amounts by applying a disbursement function to: A. the value from the first data source; and at least one of: 1. the first principal amount; and IL the second principal amount; ii. compute a second cryptographic signature from the first private key; iii. create an inchoate refund transaction record comprising: A. a commit input for receiving the commit amount from the commit transaction: B. a refund output comprising a refund amount; and C. the second cryptographic signature; and iv. publish the inchoate refund transaction record to at least one of the first client and the second client; and c. the inchoate disbursement transaction record further comprises one or more disbursement outputs comprising the disbursement amounts (0157-0174, 0176-0179, 0251, 0300, 0535, 0791-0802, 0806-0807, 0845)

38. As per claim 22

Rosen discloses where: a. the terms further comprise: a second principal amount; and ii. an expiration timestamp; b. the first key pair sector further stores a fourth asymmetric key pair, the fourth asymmetric key pair comprising a fourth private

key and a fourth public key; c. the first computer processor is further configured to: i. compute one or more disbursement amounts by applying a disbursement function to: A. the value from the first data source; and at least one of: 1. the first principal amount; and IL the second principal amount; I. read the fourth private key from the first key pair sector; iii. compute a second cryptographic signature from the fourth private key; iv. create a commit transaction record comprising: A. a first principal input for receiving the first principal amount from the first principal transaction; B. a second principal input for receiving the second principal amount from the second principal transaction; C. a commit output comprising the commit amount; and D. the second cryptographic signature; and v. create the commit transaction by submitting the commit transaction record to the transfer mechanism; and d. the inchoate disbursement transaction record further comprises one or more disbursement outputs comprising the disbursement amounts (0157-0174, 0176-0179, 0251, 0300, 0535, 0791-0802, 0806-0807).

39. As per claim 23

Rosen discloses where: a. the second computer processor is further configured to: i. compute a third cryptographic signature from the second private key; ii. create a first principal transaction record comprising: A. a first principal output comprising the first principal amount; and B. the third cryptographic signature; and iii. create a first principal transaction by submitting the first principal transaction record to the transfer mechanism; and b. the third computer processor is further configured to: i. compute a fourth cryptographic signature from the third private key; ii. create a second principal transaction record comprising: A. a second principal output comprising the second principal amount; and B. the fourth cryptographic signature; and iii. create a second

principal transaction by submitting the second principal transaction record to the transfer mechanism (0157-0174, 0176-0179, 0300, 0490, 0662, 0791-0802)

40. As per claim 24

Rosen discloses a method for facilitating value transfers via a transfer mechanism (0149-0151, 0161, Figure 56)

Rosen discloses the transfer mechanism comprising a digital currency (0118)

Rosen discloses the method comprising: a. storing a first asymmetric key pair in a first key pair sector of a first memory, the first asymmetric key pair comprising a first private key and a first public key (0162, 0685-688, claims 1, 2 and 13)

Rosen discloses b. storing a second asymmetric key pair in a second key pair sector of a second memory, the second asymmetric key pair comprising a second private key and a second public key (0142-0143, 0159, 0749, claim 91)

Rosen discloses c. storing a third asymmetric key pair in the second key pair sector, the third key pair comprising a third private key and a third public key (1660-1663, Figure 57A)

Rosen discloses d. storing a fourth asymmetric key pair in a third key pair sector of a third memory, the fourth asymmetric key pair comprising a fourth private key and a fourth public key (0193, 0683-0688, 0854, Figure 56, claim 13)

Rosen discloses e. transmitting terms from a client via a first network interface (0231-0234) the terms comprising: i. a first principal amount (0165) and ii. a reference to a first data source (0159, 1297)

Rosen discloses f. receiving the terms at a facilitator via a second network interface (0026, 0589, 0666)

Rosen discloses g. reading the first private key from the first key pair sector (0504, claim 13)

Rosen discloses h. computing a first cryptographic signature from the first private key (0660, 0662, 0702)

Rosen discloses i. creating a first principal transaction record comprising: i. a first principal output comprising the first principal amount; and ii. the first cryptographic signature (0157-0174)

Rosen discloses j. creating a first principal transaction by submitting the first principal transaction record to the transfer mechanism (0546, 0791-0802)

Rosen discloses k. reading the second private key from the second key pair sector (0630, 0664, 0749, Figure 52)

Rosen discloses l. computing a second cryptographic signature from the second private key (0660, 0662)

Rosen discloses m. creating a commit transaction record comprising: a first principal input for receiving the first principal amount from the first principal transaction; ii. a commit output comprising a commit amount; and iii. the second cryptographic signature (0157-0174, 0176-0179, 0300, 0535, 0791-0802)

Rosen discloses n. creating the commit transaction by submitting the commit transaction record to the transfer mechanism (0157-0174, 0176-0179, 0300, 0535, 0791-0802)

Rosen discloses o. retrieving a value from the first data source (0149, 0677)

Rosen discloses p. reading the third private key from the second key pair sector (0664, 1660-1663, Figure 56)

Rosen discloses q. computing a third cryptographic signature from the second private key (0157-0174, 0176-0179, 0193, 0300, 0791-0802)

Rosen discloses r. creating an inchoate disbursement transaction record comprising: i. a commit input for receiving a commit amount from a commit transaction; ii. the third cryptographic signature (0157-0174, 0176-0179, 0193, 0300, 0791-0802)

Rosen discloses s. publishing the inchoate disbursement transaction record (0157-0174, 0176-0179, 0193, 0300, 0791-0802)

Rosen discloses t, reading the inchoate disbursement transaction record (0157-0174, 0176-0179, 0193, 0300, 0660, 0662, 0791-0802)

Rosen discloses u. reading the fourth private key from the third key pair sector (0157-0174, 0176-0179, 0193, 0300, 0660, 0662, 0791-0802)

Rosen discloses v. computing a fourth cryptographic signature from the fourth private key (0157-0174, 0176-0179, 0193, 0300, 0660, 0662, 0791-0802)

Rosen discloses w. creating a complete disbursement transaction record comprising: i, the commit input; ii. the third cryptographic signature; and iii. the fourth cryptographic signature (0157-0174, 0176-0179, 0193, 0300, 0660, 0662, 0791-0802)

Rosen discloses x. creating a disbursement transaction by submitting the complete disbursement transaction record to the transfer mechanism (0157-0174, 0176-0179, 0193, 0300, 0660, 0662, 0791-0802)

Rosen, while disclosing electronic money (Abstract), does not explicitly disclose wherein the transfer mechanism comprises a decentralized currency. Feigelson teaches wherein the transfer mechanism comprises a decentralized currency (0050-0051)

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the electronic monetary system of Rosen with the creation and use of digital currency of Feigelson for the purpose of maintaining secrecy of information in order to control its value (0003).

41. As per claim 25

Rosen discloses a. computing a disbursement amount by applying a disbursement function to: L. the first principal amount; and ii. the value from the first data source; and where: b. the inchoate disbursement transaction record further comprises a disbursement output comprising the disbursement amount; and c. the complete disbursement transaction record further comprises the disbursement output (0157-0174, 0791-0802)

42. As per claim 26

Rosen discloses computing a fifth cryptographic signature from the third private key; b. creating an inchoate refund transaction record comprising: i. a commit input for receiving the commit amount from the commit transaction; ii. a refund output comprising a refund amount; iii. the fifth cryptographic signature; and iv. a lock time; and c. publishing the inchoate refund transaction record (0157-0174, 0176-0179, 0251, 0300, 0660, 0662, 0806-0807, 0845)

43. As per claim 27

Rosen discloses where at least one of: a. the second asymmetric key pair consists of the third asymmetric key pair, the second private key consists of the third private key, and the second public key consists of the third public key; b. the first asymmetric key pair consists of the fourth asymmetric key pair, the first private key

consists of the fourth private key, and the first public key consists of the fourth public key; and c. the first memory consists of the third memory and the first key pair sector consists of the third key pair sector (claims 1, 2 and 13)

44. As per claim 28

Rosen discloses storing a fifth asymmetric key pair in a fourth key pair sector of a fourth memory, the fifth asymmetric key pair comprising a fifth private key and a fifth public key; b. reading the fifth private key from the fourth key pair sector; c. computing a fifth cryptographic signature from the fifth private key; d. creating a second principal transaction record comprising: i. a second principal output comprising the second principal amount; and ii. the fifth cryptographic signature; e. creating a second principal transaction by submitting the second principal transaction record to the transfer mechanism; f. computing one or more disbursement amounts by applying a disbursement function to: i. the value from the first data source; and at least one of: A. the first principal amount; and B. the second principal amount; and where: g. the inchoate disbursement transaction record further comprises one or more disbursement outputs comprising the disbursement amounts; and h. the complete disbursement transaction record further comprises the disbursement outputs (0157-0174, 0176-0179, 0288, 0504, 0535, 0546, 0791-0802)

45. As per claim 29

Rosen discloses a. computing a sixth cryptographic signature from the third private key; b. creating an inchoate refund transaction record comprising: L. a commit input for receiving the commit amount from the commit transaction; ii. one or more refund outputs comprising one or more refund amounts; iii. the sixth cryptographic

signature; and iv. a lock time; and c. publishing the inchoate refund transaction record (0157-0174, 0176-0179, 0251, 0300, 0660, 0662, 0806-0807, 0845)

46. As per claim 30

Rosen discloses where at least one of: a. the second asymmetric key pair consists of the third asymmetric key pair, the second private key consists of the third private key, and the second public key consists of the third public key; b. the first asymmetric key pair consists of the fourth asymmetric key pair, the first private key consists of the fourth private key, and the first public key consists of the fourth public key; c. the fifth asymmetric key pair consists of the fourth asymmetric key pair, the fifth private key consists of the fourth private key, and the fifth public key consists of the fourth public key; d. the first memory consists of the third memory and the first key pair sector consists of the third key pair sector; and e. the fifth memory consists of the third memory and the fifth key pair sector consists of the third key pair sector (claim 1, claim 2 and claim 13).

Conclusion

47. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JAMES D NIGH whose telephone number is (571)270-5486. The examiner can normally be reached on 6-9 AM and 11 AM TO 4 PM.

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, Neha Patel can be reached on (571) 270-1492. 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.

/JAMES D NIGH/
Primary Examiner, Art Unit 3685

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/309,612	Middleton et al.
	Examiner	Art Unit
	JAMES D NIGH	3685

CPC - Searched*		
Symbol	Date	Examiner

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
EAST Text Search	07/18/2019	JDN

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

	/JAMES D NIGH/ Primary Examiner, Art Unit 3685

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	5	("20030070080" | "20130054471" | "20130166455" | "20130179337" | "20130212388").PN.	US-PGPUB; USPAT	AND	ON	2019/07/18 07:53
S2	17	(server near20 ("public key") near20 ("private key")) ((transaction or principal) near10 amount) (signature near20 "private key") ((client or agent) near20 "private key") ((digital or electronic) near10 currency) @ad<="20140509"	US-PGPUB; USPAT	AND	ON	2019/07/18 08:22

7/ 20/ 2019 3:13:03 PM
C:\ Users\ jnigh\ Documents\ EAST\ Workspaces\ 15309612.wsp

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 15/309,612	Filing Date 11/08/2016	☐ 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 $40 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $210 =	
☐ 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	10/24/2019	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 30	Minus	** 30	= 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".	/TONI R HAKIM/
*** 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

Application Serial No..... 15/309,612
Filing Date ..... November 08, 2016
Confirmation No. 2321
Inventorship ..... Reginald Middleton
Group Art Unit..... 3685
Examiner .....NIGH, JAMES D
Attorney Docket No. 4675.1002BS
Title: .....Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers

RESPONSE TO NON-FINAL OFFICE ACTION OF JULY 24, 2019

To: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

From: Misung Lee
Customer No. 86636
Brundidge & Stanger, PC
1925 Ballenger Ave., Suite 560
Alexandria, VA 22314

Sir:

In response to the Non-final Office Action dated July 24, 2019, for which the three-month shortened statutory period for response is set to expire on October 24, 2019, the following amendments and remarks are respectfully submitted. Favorable consideration is respectfully requested.

The Commissioner is hereby authorized to charge any deficiency of fees and credit any overpayments to Deposit Account Number 50-4888.

INTRODUCTORY COMMENTS

The Listing of the Claims section begins on page 3.

Remarks section begins on page 22.

LISTING OF THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Claims pending:

- At time of the Action: **Claims 1-30**
- After this Reply: **Claims 1-30**

Currently Canceled or Withdrawn Claims: None

Currently Amended Claims: **Claims 1, 3-5, and 7-30**

New Claims: None

1. (**Currently Amended**) A device for facilitating a value transfer between a first party utilizing a first client and a second party utilizing a second client via a transfer mechanism, the device comprising:

~~a.~~ a first memory comprising a transaction record sector and a first key pair sector for storing a first asymmetric key pair, the first asymmetric key pair comprising a first private key and a first public key;

~~b.~~ a first network interface for receiving terms, the terms comprising:

~~i.~~ a first principal amount; and

~~ii.~~ a reference to a first data source; and

~~c.~~ a first computer processor coupled to the first memory and the first network interface, the first computer processor configured to:

~~i.~~ retrieve a value from the first data source;

~~ii.~~ read the first private key from the first key pair sector;

~~iii.~~ compute a first cryptographic signature from the first private key;

~~iv.~~ create an inchoate disbursement transaction record comprising:

~~A.~~ a commit input for receiving a commit amount from a commit transaction; and

~~B.~~ the first cryptographic signature; and

~~v.~~ publish the inchoate disbursement transaction record to at least one of the first client and the second client;

where the first client comprises:

~~a.~~ a second memory comprising a second key pair sector for storing a second asymmetric key pair, the second asymmetric key pair comprising a second private key and a second public key;

~~b.~~ a second network interface; and

~~c.~~ a second computer processor coupled to the second memory and the second network interface, the second computer processor configured to read the second private key from the second key pair sector; and

where the second client comprises;

~~a.~~ a third memory comprising a third key pair sector for storing a third asymmetric key pair, the third asymmetric key pair comprising a third private key and a third public key;

~~b.~~ a third network interface; and

~~c.~~ a third computer processor coupled to the third memory and the third network interface, the third computer processor configured to read the third private key from the third key pair sector.

2. (**Original**) The device of claim 1, where the transfer mechanism comprises a decentralized digital currency.

3. (**Currently Amended**) The device of claim 1, where:

~~a.~~ the first computer processor is further configured to compute a disbursement amount by applying a disbursement function to:

~~i.~~ the first principal amount; and

~~ii~~. the value from the first data source; and

~~b.~~ the inchoate disbursement transaction record further comprises a disbursement output comprising the disbursement amount.

4. (**Currently Amended**) The device of claim 3, where the first computer processor is further configured to:

~~a.~~ compute a second cryptographic signature from the first private key;

~~b.~~ create an inchoate refund transaction record comprising:

~~i.~~ a commit input for receiving the commit amount from the commit transaction;

~~ii.~~ a refund output comprising a refund amount;

~~iii.~~ the second cryptographic signature; and

~~iv.~~ a lock time; and

~~c.~~ publish the inchoate refund transaction record to at least one of the first client or the second client.

5. (**Currently Amended**) The device of claim 3, where:

~~a.~~ the first key pair sector further stores a fourth asymmetric key pair, the fourth asymmetric key pair comprising a fourth private key and a fourth public key; and

~~b.~~ the first computer processor is further configured to:

~~i.~~ read the fourth private key from the first key pair sector;

~~ii.~~ compute a second cryptographic signature from the fourth private key;

~~iii.~~ create a commit transaction record, the commit transaction record comprising:

~~A.~~ a first principal input for receiving the first principal amount from a first principal transaction;

~~B.~~ a commit output comprising the commit amount;

~~C.~~ the second cryptographic signature; and

~~iv.~~ create the commit transaction by submitting the commit transaction record to the transfer mechanism.

6. (**Original**) The device of claim 5, where the first asymmetric key pair consists of the fourth asymmetric key pair, the first private key consists of the fourth private key, and the first public key consists of the fourth public key.

7. (**Currently Amended**) The device of claim 1, where:

~~a.~~ the terms further comprise:

~~i.~~ a second principal amount; and

~~ii.~~ an expiration timestamp;

~~b.~~ the first computer processor is further configured to compute the one or more disbursement amounts by applying a disbursement function to:

~~i.~~ the value from the first data source; and at least one of:

~~A.~~ the first principal amount; and

~~B.~~ the second principal amount; and

~~c.~~ the inchoate disbursement transaction record further comprises one or more disbursement outputs comprising the disbursement amounts.

8. (**Currently Amended**) The device of claim 7, where:

~~a.~~ the terms further comprise:

~~i.~~ a reference to a second data source;

~~b.~~ the first computer processor is further configured to compute the one or more disbursement amounts by applying the disbursement function to:

~~i.~~ the value from the first data source;

~~ii.~~ the value from the second data source;

~~iii.~~ the first principal amount; and

~~iv.~~ the second principal amount.

9. (**Currently Amended**) The device of claim 7, where:

~~a.~~ the reference to the first data source comprises at least one of a reference to a base instrument and a reference to a quote instrument; and

~~b.~~ the first computer processor is further configured to compute the disbursement amounts on or after the expiration timestamp.

10. (**Currently Amended**) The device of claim 7, where the first computer processor is further configured to:

~~a.~~ compute a second cryptographic signature from the first private key;

~~b.~~ create an inchoate refund transaction record comprising:

~~i.~~ a commit input for receiving the commit amount from the commit transaction;

~~ii.~~ one or more refund outputs comprising one or more refund amounts;

~~iii.~~ the second cryptographic signature; and

~~iv.~~ a lock time; and

~~c.~~ publish the inchoate refund transaction record to at least one of the first client and the second client.

11. (**Currently Amended**) The device of claim 7, where:

~~a.~~ the first key pair sector further stores a fourth asymmetric key pair, the fourth asymmetric key pair comprising a fourth private key and a fourth public key; and

~~b.~~ the first computer processor is further configured to:

~~i.~~ read the fourth private key from the first key pair sector;

~~ii.~~ compute a second cryptographic signature from the fourth private key;

~~iii.~~ create a commit transaction record comprising:

~~A.~~ a first principal input for receiving the first principal amount from a first principal transaction;

~~B.~~ a second principal input for receiving the second principal amount from a second principal transaction;

~~C.~~ a commit output comprising a commit amount; and

~~D.~~ the second cryptographic signature; and

~~iv.~~ create the commit transaction by submitting the commit transaction record to the transfer mechanism.

12. (**Currently Amended**) A system for facilitating a value transfer between a first party utilizing a first client and a second party utilizing a second client via a transfer mechanism, the transfer mechanism comprising a decentralized digital currency, the system comprising a facilitator, the first client, and the second client;

~~a.~~ the facilitator comprising:

i. a first memory comprising a transaction record sector and a first key pair sector for storing a first asymmetric key pair, the first asymmetric key pair comprising a first private key and a first public key;

ii. a first network interface for receiving terms, the terms comprising:

A. a first principal amount; and

B. a reference to a first data source; and

iii. a first computer processor coupled to the first memory and the first network interface, the first computer processor configured to:

A. retrieve a value from the first data source;

B. read the first private key from the first key pair sector;

C. compute a first cryptographic signature from the first private key;

D. create an inchoate disbursement transaction record comprising:

I. a commit input for receiving a commit amount from a commit transaction; and

II. the first cryptographic signature; and

E. publish the inchoate disbursement transaction record to at least one of the first client and the second client;

b. the first client comprising:

i. a second memory comprising a second key pair sector for storing a second asymmetric key pair, the second asymmetric key pair comprising a second private key and a second public key;

ii. a second network interface; and

~~iii.~~ a second computer processor coupled to the second memory and the second network interface, the second computer processor configured to read the second private key from the second key pair sector; and

~~c.~~ the second client comprising:

~~i.~~ a third memory comprising a third key pair sector for storing a third asymmetric key pair, the third asymmetric key pair comprising a third private key and a third public key;

~~ii.~~ a third network interface; and

~~iii.~~ a third computer processor coupled to the third memory and the third network interface, the third computer processor configured to read the third private key from the third key pair sector.

13. (**Currently Amended**) The system of claim 12, where:

the facilitator and the first client are the same device;

~~a.~~ the first computer processor ~~consists of~~ and the second computer processor are the same processor;

~~b.~~ the first memory ~~consists of~~ and the second memory are the same memory; and

~~c.~~ the first network interface ~~consists of~~ and the second network interface are the same network interface.

14. (**Currently Amended**) The system of claim 12, where:

~~a.~~ the first computer processor is further configured compute a disbursement amount by applying a disbursement function to:

~~i.~~ the first principal amount; and

~~ii.~~ the value from the first data source;

~~b.~~ the inchoate disbursement transaction record further comprises a disbursement output comprising the disbursement amount; and

~~c.~~ the second computer processor is further configured to:

~~i.~~ read the inchoate disbursement transaction;

~~ii.~~ compute a second cryptographic signature from the second private key;

~~iii.~~ create a complete disbursement transaction record comprising:

~~A.~~ the commit input;

~~B.~~ the disbursement output;

~~C.~~ the first cryptographic signature; and

~~D.~~ the second cryptographic signature; and

~~iv.~~ create a disbursement transaction by submitting the complete disbursement transaction record to the transfer mechanism.

15. (**Currently Amended**) The system of claim 12, where the first computer processor is further configured to:

~~a.~~ compute a second cryptographic signature from the first private key;

~~b.~~ create an inchoate refund transaction record comprising:

~~i.~~ a commit input for receiving the commit amount from the commit transaction;

~~ii.~~ a refund output comprising a refund amount; and

~~iii.~~ the second cryptographic signature; and

~~c.~~ publish the inchoate refund transaction record to at least one of the first client and the second client.

16. (**Currently Amended**) The system of claim 12, where:

~~a.~~ the first key pair sector further stores a fourth asymmetric key pair, the fourth asymmetric key pair comprising a fourth private key and a fourth public key;

~~b.~~ the first computer processor is further configured to:

~~i.~~ compute a disbursement amount by applying a disbursement function to:

~~A.~~ the first principal amount; and

~~B.~~ the value from the first data source;

~~ii.~~ read the fourth private key from the first key pair sector;

~~iii.~~ compute a second cryptographic signature from the fourth private key;

~~iv.~~ create a commit transaction record comprising:

~~A.~~ a first principal input for receiving the first principal amount from a first principal transaction;

~~B.~~ a commit output comprising the commit amount; and

~~C.~~ the second cryptographic signature; and

~~v.~~ create the commit transaction by submitting the commit transaction record to the transfer mechanism; and

~~c.~~ the inchoate disbursement transaction record further comprises a disbursement output comprising the disbursement amount.

17. (**Currently Amended**) The system of claim 16, where the second computer processor is configured to:

~~a.~~ compute a third cryptographic signature from the second private key;

~~b.~~ create a first principal transaction record comprising:

~~i.~~ a first principal output comprising the first principal amount; and

~~ii.~~ the third cryptographic signature; and

~~c.~~ create the first principal transaction by submitting the first principal transaction record to the transfer mechanism.

18. (**Currently Amended**) The system of claim 12, where:

~~a.~~ the terms further comprise:

~~i.~~ a second principal amount; and

~~ii.~~ an expiration timestamp;

~~b.~~ the first computer processor is further configured compute one or more disbursement amounts by applying a disbursement function to:

~~i.~~ the value from the first data source; and at least one of:

~~A.~~ the first principal amount; and

~~B.~~ the second principal amount;

~~c.~~ the inchoate disbursement transaction record further comprises one or more disbursement outputs comprising the disbursement amounts; and

~~d.~~ the second computer processor is further configured to:

~~i.~~ read the inchoate disbursement transaction;

~~ii.~~ compute a second cryptographic signature from the second private key;

~~iii.~~ create a complete disbursement transaction record comprising:

~~A.~~ the commit input;

~~B.~~ the disbursement outputs;

~~C.~~ the first cryptographic signature; and

~~D.~~ the second cryptographic signature; and

~~iv.~~ create a disbursement transaction by submitting the complete disbursement transaction record to the transfer mechanism.

19. (**Currently Amended**) The system of claim 18, where:

~~a.~~ the terms further comprise:

~~i.~~ a reference to a second data source;

~~b.~~ the first computer processor is further configured to compute the one or more disbursement amounts by applying the disbursement function to:

~~i.~~ the value from the first data source;

~~ii.~~ the value from the second data source;

~~iii.~~ the first principal amount; and

~~iv.~~ the second principal amount.

20. (**Currently Amended**) The system of claim 18, where:

~~a.~~ the reference to the first data source comprises at least one of a reference to a base instrument and a reference to a quote instrument; and

~~b.~~ the first computer processor is further configured to compute the disbursement amounts on or after the expiration timestamp.

21. (**Currently Amended**) The system of claim 12, where:

~~a.~~ the terms further comprise:

~~i.~~ a second principal amount; and

~~ii.~~ an expiration timestamp;

~~b.~~ the first computer processor is further configured to:

~~i.~~ compute one or more disbursement amounts by applying a disbursement function to:

~~A.~~ the value from the first data source; and at least one of:

I. the first principal amount; and

II. the second principal amount;

ii. compute a second cryptographic signature from the first private key;

iii. create an inchoate refund transaction record comprising:

A. a commit input for receiving the commit amount from the commit transaction;

B. a refund output comprising a refund amount; and

C. the second cryptographic signature; and

iv. publish the inchoate refund transaction record to at least one of the first client and the second client; and

c. the inchoate disbursement transaction record further comprises one or more disbursement outputs comprising the disbursement amounts.

22. (**Currently Amended**) The system of claim 12, where:

a. the terms further comprise:

i. a second principal amount; and

ii. an expiration timestamp;

b. the first key pair sector further stores a fourth asymmetric key pair, the fourth asymmetric key pair comprising a fourth private key and a fourth public key;

c. the first computer processor is further configured to:

i. compute one or more disbursement amounts by applying a disbursement function to:

A. the value from the first data source; and at least one of:

I. the first principal amount; and

II. the second principal amount;

~~ii.~~ read the fourth private key from the first key pair sector;

~~iii.~~ compute a second cryptographic signature from the fourth private key;

~~iv.~~ create a commit transaction record comprising:

~~A.~~ a first principal input for receiving the first principal amount from the first principal transaction;

~~B.~~ a second principal input for receiving the second principal amount from the second principal transaction;

~~C.~~ a commit output comprising the commit amount; and

~~D.~~ the second cryptographic signature; and

~~v.~~ create the commit transaction by submitting the commit transaction record to the transfer mechanism; and

~~d.~~ the inchoate disbursement transaction record further comprises one or more disbursement outputs comprising the disbursement amounts.

23. (**Currently Amended**) The system of claim 22, where:

~~a.~~ the second computer processor is further configured to:

~~i.~~ compute a third cryptographic signature from the second private key;

~~ii.~~ create a first principal transaction record comprising:

~~A.~~ a first principal output comprising the first principal amount; and

~~B.~~ the third cryptographic signature; and

~~iii.~~ create a first principal transaction by submitting the first principal transaction record to the transfer mechanism; and

~~b.~~ the third computer processor is further configured to:

~~i.~~ compute a fourth cryptographic signature from the third private key;

ii. create a second principal transaction record comprising:

A. a second principal output comprising the second principal amount; and

B. the fourth cryptographic signature; and

iii. create a second principal transaction by submitting the second principal transaction record to the transfer mechanism.

24. (**Currently Amended**) A method for facilitating value transfers via a transfer mechanism, the transfer mechanism comprising a decentralized digital currency, the method comprising:

a. storing a first asymmetric key pair in a first key pair sector of a first memory, the first asymmetric key pair comprising a first private key and a first public key;

b. storing a second asymmetric key pair in a second key pair sector of a second memory, the second asymmetric key pair comprising a second private key and a second public key;

c. storing a third asymmetric key pair in the second key pair sector, the third key pair comprising a third private key and a third public key;

d. storing a fourth asymmetric key pair in a third key pair sector of a third memory, the fourth asymmetric key pair comprising a fourth private key and a fourth public key;

e. transmitting terms from a client via a first network interface, the terms comprising:

i. a first principal amount; and

ii. a reference to a first data source;

f. receiving the terms at a facilitator via a second network interface;

g. reading the first private key from the first key pair sector;

h. computing a first cryptographic signature from the first private key;

i. creating a first principal transaction record comprising:

i. a first principal output comprising the first principal amount; and

ii. the first cryptographic signature;

j. creating a first principal transaction by submitting the first principal transaction record to the transfer mechanism;

k. reading the second private key from the second key pair sector;

l. computing a second cryptographic signature from the second private key;

m. creating a commit transaction record comprising:

i. a first principal input for receiving the first principal amount from the first principal transaction;

ii. a commit output comprising a commit amount; and

iii. the second cryptographic signature;

n. creating the commit transaction by submitting the commit transaction record to the transfer mechanism;

o. retrieving a value from the first data source;

p. reading the third private key from the second key pair sector;

q. computing a third cryptographic signature from the second private key;

r. creating an inchoate disbursement transaction record comprising:

i. a commit input for receiving a commit amount from a commit transaction;

ii. the third cryptographic signature;

s. publishing the inchoate disbursement transaction record;

t. reading the inchoate disbursement transaction record;

u. reading the fourth private key from the third key pair sector;

v. computing a fourth cryptographic signature from the fourth private key;

w. creating a complete disbursement transaction record comprising:

i. the commit input;

~~ii.~~ the third cryptographic signature; and

~~iii.~~ the fourth cryptographic signature; and

~~x.~~ creating a disbursement transaction by submitting the complete disbursement transaction record to the transfer mechanism.

25. (**Currently Amended**) The method of claim 24, further comprising ~~the steps~~:

~~a.~~ computing a disbursement amount by applying a disbursement function to:

~~i.~~ the first principal amount; and

~~ii.~~ the value from the first data source; and

where:

~~b.~~ the inchoate disbursement transaction record further comprises a disbursement output comprising the disbursement amount; and

~~c.~~ the complete disbursement transaction record further comprises the disbursement output.

26. (**Currently Amended**) The method of claim 25, further comprising ~~the steps~~:

~~a.~~ computing a fifth cryptographic signature from the third private key;

~~b.~~ creating an inchoate refund transaction record comprising:

~~i.~~ a commit input for receiving the commit amount from the commit transaction;

~~ii.~~ a refund output comprising a refund amount;

~~iii.~~ the fifth cryptographic signature; and

~~iv.~~ a lock time; and

~~c.~~ publishing the inchoate refund transaction record.

27. (**Currently Amended**) The method of claim 25, where at least one of:

~~a.~~ the second asymmetric key pair consists of the third asymmetric key pair, the second private key consists of the third private key, and the second public key consists of the third public key;

~~b.~~ the first asymmetric key pair consists of the fourth asymmetric key pair, the first private key consists of the fourth private key, and the first public key consists of the fourth public key; ~~and~~or

~~c.~~ the first memory ~~consists of~~and the third memory are the same memory, and the first key pair sector consists of the third key pair sector.

28. (**Currently Amended**) The method of claim 24, further comprising ~~the steps~~:

~~a.~~ storing a fifth asymmetric key pair in a fourth key pair sector of a fourth memory, the fifth asymmetric key pair comprising a fifth private key and a fifth public key;

~~b.~~ reading the fifth private key from the fourth key pair sector;

~~c.~~ computing a fifth cryptographic signature from the fifth private key;

~~d.~~ creating a second principal transaction record comprising:

~~i.~~ a second principal output comprising the second principal amount; and

~~ii.~~ the fifth cryptographic signature;

~~e.~~ creating a second principal transaction by submitting the second principal transaction record to the transfer mechanism;

~~f.~~ computing one or more disbursement amounts by applying a disbursement function to:

~~i.~~ the value from the first data source; and at least one of:

~~A.~~ the first principal amount; and

~~B.~~ the second principal amount; and

where:

~~g.~~ the inchoate disbursement transaction record further comprises one or more disbursement outputs comprising the disbursement amounts; and

~~h.~~ the complete disbursement transaction record further comprises the disbursement outputs.

29. (**Currently Amended**) The method of claim 28, further comprising ~~the steps~~:

~~a.~~ computing a sixth cryptographic signature from the third private key;

~~b.~~ creating an inchoate refund transaction record comprising:

~~i.~~ a commit input for receiving the commit amount from the commit transaction;

~~ii.~~ one or more refund outputs comprising one or more refund amounts;

~~iii.~~ the sixth cryptographic signature; and

~~iv.~~ a lock time; and

~~c.~~ publishing the inchoate refund transaction record.

30. (**Currently Amended**) The method of claim 28, where at least one of:

~~a.~~ the second asymmetric key pair consists of the third asymmetric key pair, the second private key consists of the third private key, and the second public key consists of the third public key;

~~b.~~ the first asymmetric key pair consists of the fourth asymmetric key pair, the first private key consists of the fourth private key, and the first public key consists of the fourth public key;

~~c.~~ the fifth asymmetric key pair consists of the fourth asymmetric key pair, the fifth private key consists of the fourth private key, and the fifth public key consists of the fourth public key;

~~d.~~ the first memory ~~consists of~~and the third memory are the same memory and the first key pair sector consists of the third key pair sector; ~~and~~or

~~e.~~ the ~~fifth~~ fourth memory ~~consists of~~ and the third memory are the same memory, and the ~~fifth~~ fourth key pair sector consists of the third key pair sector.

Electronic Acknowledgement Receipt

EFS ID:	37547440
Application Number:	15309612
International Application Number:	
Confirmation Number:	2321
Title of Invention:	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers
First Named Inventor/Applicant Name:	Reginald Middleton
Customer Number:	86636
Filer:	Misung Lee/Mariah Duell
Filer Authorized By:	Misung Lee
Attorney Docket Number:	4675.1002BS
Receipt Date:	24-OCT-2019
Filing Date:	08-NOV-2016
Time Stamp:	11:49:29
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	Amendment/Req. Reconsideration-After Non-Final Reject	4675_Response.pdf	187068 5557f9566083a795243be1f2850b7519491b2c5c	no	30

Warnings:

Information:	
Total Files Size (in bytes):	187068

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.

REMARKS

Reconsideration and allowance in view of the foregoing amendments and the following remarks are respectfully requested.

Claims 1-30 are pending. **Claims 13, 27, and 30** were rejected under 35 U.S.C. § 112(b)/112(d). **Claims 13, 27, and 30** were rejected under 35 U.S.C. § 102(a)(1)/(a)(2). **Claims 12-30** were rejected under 35 U.S.C. § 103(a). Upon entry of the amendment, **Claims 1, 3-5, and 7-30** are currently amended. Support for the amendments to **Claims 13, 17, and 30** can be found, at least at, paragraph [0055] of the U.S. Patent Application Publication. No new matter is added.

Favorable consideration is respectfully requested.

CLAIM REJECTION UNDER 35 U.S.C. § 112

Claims 13, 27, and 30 *are rejected under 35 U.S.C. § 112(b) or 35 U.S.C. § 112 (pre-AIA), second paragraph, as allegedly 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.*

Claims 13, 27, and 30 *are rejected under 35 U.S.C. § 112(d) or pre-AIA 35 U.S.C. § 112, 4th paragraph, as allegedly being of improper dependent form for failing to further limit the subject matter of the claim upon which it depends, or for failing to include all the limitations of the claim upon which it depends.*

Applicant is currently amending **Claims 13, 17, and 30** to address the rejections. Support for the amendments can be found, at least at, paragraph [0055] of the U.S. Patent Application Publication. Accordingly, it is respectfully requested that the rejections under 35 U.S.C. §§ 112(b) and 112(d) to the claims be reconsidered and withdrawn.

CLAIM REJECTION UNDER 35 U.S.C. § 102(a)(1) and (a)(2)

Claims 1 and 3-11 *are rejected under 35 U.S.C. §§ 102(a)(1) and 102(a)(2) as allegedly being anticipated by Rosen (U.S. Publication No. 2003/0070080; hereafter "Rosen").*

Applicant traverses the rejections, and respectfully requests that the rejections be reconsidered and withdrawn.

Claim 1 recites, in part (emphasis added):

> **A device for facilitating a value transfer** between a first party utilizing a first client and a second party utilizing a second client via a transfer mechanism, the device comprising:
>
> **a first memory comprising a transaction record sector and a first key pair sector for storing a first asymmetric key pair, the first asymmetric key pair comprising a first private key and a first public key**;
>
> a first network interface for receiving terms, the terms comprising:
>
> a first principal amount; and
>
> a reference to a first data source; and
>
> **a first computer processor** coupled to the first memory and the first network interface, the first computer processor configured to:
>
> retrieve a value from the first data source;
>
> **read the first private key from the first key pair sector;**
>
> **compute a first cryptographic signature from the first private key;**
>
> **create an inchoate disbursement transaction record comprising:**
>
> **a commit input for receiving a commit amount from a commit transaction; and**
>
> **the first cryptographic signature; and**
>
> **publish the inchoate disbursement transaction record to at least one of the first client and the second client**...

In the rejection of **Claim 1**, the Office Action, at page 5, alleges (emphasis added):

> Rosen discloses a first memory comprising **a transaction record sector and a first key pair sector for storing a first asymmetric key pair, the first asymmetric key pair comprising a first private key and a first public key** (0162 "**The Tran Log Mgr. application 36** provides the management and overseeing of a log that records completed transactions undertaken by the money module", 0685-0688 **"Each primary trusted server 210 has its own public key and corresponding private key"**, claim 1, claim 2, claim 13)

Applicant respectfully disagrees.

Paragraphs [0162], and [0685]-[0688] of Rosen state:

[0162] **The Tran Log Mgr. application 36 provides the management and overseeing of a log that records completed transactions undertaken by the money module.** For each completed transfer of electronic money, an illustrative Tran Log records:

[0685] **Each primary trusted server 210 has its own public key and corresponding private key.** The primary trusted server public keys are commonly shared by all trusted servers 200 and trusted agents 120 in the system. These public keys are stored in a primary trusted server public key (PTS(PK)) list. The term "public" key as used here and throughout the specification, does not imply that the key is known to the public at large. In this case, for example, the public key is known only to all trusted servers 200 and trusted agents 120 and is sealed within their tamper-proof housings. This limited sense of "public" provides added security to the system as a whole

[0686] Beneath the primary trusted server 210 on the security hierarchy are the trusted servers 200 which may be located throughout the overall commerce system. The trusted servers 200 provide trusted agent certificates (cert(TA)) to the trusted agents 120 (i.e., CTAs 2, MTAs 4, and ATAs 212).

[0687] The Trusted Agency guarantees the protocols and physical protection of each trusted agent 120 in the system. Trusted agents 120 are manufactured in a physically secure environment under control of the Trusted Agency. The components are fabricated, assembled, and loaded with software in this environment. The trusted agents 120 are then tamper-proofed and can only be communicated with through their external interface.

[0688] At initialization, each trusted agent 120 is placed in communication with a trusted server 200. The trusted server 200 assigns each trusted agent 120 a unique identification number TA(id). Then the trusted server 200 requests the trusted agent 120 to generate a public and private key pair. The trusted agent 120 generates the key pair and passes its public key (TA(PK)) to the requesting trusted server 200. The trusted server 200 incorporates this information and the TA(id) into a trusted agent certificate cert(TA) and passes it back to the trusted agent 120 along with a PTS(PK) list, and an untrusted list. Finally, the trusted agent 120 tests its newly received certificate and makes sure the certificate is valid.

As context for the "Tran Log Mgr. application 36," as shown in FIG. 4 of Rosen, the Tran Log Mgr. application 36 is implemented on a Transaction money module associated with a payee (Rosen, paragraph [0131]). However, the "primary trusted server 210" as described by Rogen is another entity

separate from the Transaction money module (on which the Tran Log Mgr. application 36 is implemented), and the separate primary trusted server 210 certifies and provides trusted server certificates to trusted servers and trusted agents. Therefore, Rogen fails to describe the Transaction money module comprises both of "a transaction record sector and a first key pair sector," implemented on one entity as claimed. Accordingly, Rogen fails to teach or suggest **the device** comprising..."**a first memory comprising a transaction record sector and a first key pair sector** for storing a first asymmetric key pair, the first asymmetric key pair comprising a first private key and a first public key," as recited in **Claim 1**. Also, it naturally follows that Rogen fails to teach or suggest "the first computer processor configured to... read the first private key **from the first key pair sector**," as recited in **Claim 1**.

The Office Action, at pages 5 and 6, further alleges that:

> Rosen discloses create an inchoate disbursement transaction record comprising: a commit input for receiving a commit amount from a commit transaction (0157, 0546, 1941)
> Rosen discloses the first cryptographic signature (1946)
> Rosen discloses publish the inchoate disbursement transaction record to at least one of the first client and the second client (0142-0143, 0588-0591, Figure 3, Figure 7, Figure 36A)

Applicant respectfully disagrees.

Rosen, at paragraphs [0157], [0546], [1941], and [1946] states (emphasis added):

> [0157] Referring now to FIG. 4, a Transaction money module 4 is shown diagrammatically in block form. Specifically, a Transaction money module 4 has (1) an external interface 30 that interfaces the Transaction money module 4 to the module's data processing means, the input/output means (human interface) and the communications circuitry of the external device; (2) a session manager 31 to control and commit (i.e., finalize) or abort a transaction session; (3) a transactor 32 to manage application functions; and (4) a money holder 38 to contain and manage the electronic representations of money.
>
> [0546] Finally, to successfully complete the withdrawal of **electronic notes 11**, the money modules will "commit" to or finalize the transaction by utilizing the following procedure. Referring now to FIG. 41 for a detailed description of this process, **the Tran Log Mgr. application 31 updates its Tran Log to record the transaction that has**

> **occurred above** (Step 690). When it is a Transaction money module 4 that is committing to the exchange (Step 691), the To Subscriber application will notify the subscriber that the transaction has been successfully completed (Step 692). Of course, the Session Manager application A 31 will note the end of session (Step 693), and employ process Steps 2-8 to send the message to the money module it is transacting with.
>
> [1941] If funds are sufficient, then Pay/Exchange A passes the amount to the money holder (step 1810). The **notes** are then transferred from A to B (step 1812). Finally, the transaction money modules commit (step 1814).
>
> [1946] If the account links are correct, then the CSM 1192 sends the account profile to the security server 1184 (step 1844). **The security server 1184 digitally signs the new (or updated) profile (step 1846). The security server 1184 then sends the signed profile to the money module 1186 (step 1848).** Finally, the money module to security server transaction commits (step 1850) and the security server to CSM transaction commits (step 1852).

As set forth above, Rosen merely describes processes for completing the withdrawal of electronic notes transferred to Transaction money module 4 by committing or finalizing the transaction. As context for the electronic notes as described by Rosen, paragraph [0118] of Rosen is reproduced below.

> [0118] **Electronic notes 11, the media for transferring electronic money, are generated by the Money Generator module 6 for an Issuing Bank 1**. These notes 11 are then transferred by a Teller money module 5 to a subscriber utilizing a Transaction money module 4. **Electronic notes 11 may be representations of currency or credit authorizations.** For security reasons, all electronic notes 11 will expire after a preset time period. Once expired, the notes 11 must be redeemed at a participating bank for updated ones before they can be transferred.

As described above, the electronic notes 11 of Rosen are the media for transferring electronic money and representations of currency or credit authorizations. The electronic notes 11 are utilized to finalize or commit the transaction, and the Tran Log Mgr. application 31 updates its Tran Log to record the transaction that has occurred. However, nowhere in Rosen is there any teaching or suggestion of

"inchoate" electronic notes that is utilized to create "complete" electronic notes. That is, the electronic notes of Rosen are complete notes record that creates the transaction. Further, any log updated by the Tran Log Mgr. application 31 of Rosen is a record about the completed transaction that is updated after the transaction occurred. Therefore, the electronic notes 11 of Rosen do not teach or suggest "**an inchoate disbursement transaction record,"** as recited in **Claim 1.**

Furthermore, electronic notes of Rosen are generated by the Money Generator module 6 but not by the "PAY/EXCHANGE application 35" implemented on Transaction money module 4 (which allegedly corresponds to the device for facilitating a value transfer by page 4 of the Office Action). Therefore, Rosen fails to teach or suggest "**a first computer processor**" [of the device for facilitating a value transfer] configured to "**create an inchoate disbursement transaction record**," as recited in **Claim 1**.

Further still, Rosen, at paragraph [1946], describes that the security server 1184 digitally signs the new (or updated) profile and then sends the signed profile to the money module. That is, Rosen describes the digitally signed profile is computed by the security server which is another entity separated from the money module. Therefore, Rosen fails to teach or suggest "**a first computer processor**" [of the device for facilitating a value transfer] configured to create an inchoate disbursement transaction record comprising... "the first cryptographic signature" [that is computed by the first computer processor], as recited in **Claim 1**.

Accordingly, Rosen fails to teach or suggest at least below emphasized features of **Claim 1**:

> **a first computer processor** coupled to the first memory and the first network interface, the first computer processor configured to:
> retrieve a value from the first data source;
> **read the first private key from the first key pair sector;**
> **compute a first cryptographic signature from the first private key;**
> **create an inchoate disbursement transaction record comprising:**
> **a commit input for receiving a commit amount from a commit transaction; and**

the first cryptographic signature; and
publish the inchoate disbursement transaction record
to at least one of the first client and the second client...

Claims 3-11 variously depend, directly or indirectly, from independent **Claim 1**. Rosen is deficient with respect to independent **Claim 1,** for at least the reasons stated above. Therefore, Applicant submits that **Claims 3-11** are patentable over Rosen at least by virtue of their dependency, as well as the other features recited therein. Applicant, therefore respectfully requests the reconsideration and withdrawal of rejections under 35 U.S.C. § 102(a)(1) and 102(a)(b).

CLAIM REJECTION UNDER 35 U.S.C. § 103

Claims 2 and 12-30 *are rejected under 35 U.S.C. § 103 as allegedly being unpatentable over Rosen, in view of Feigelson (U.S. Publication No. 2013/0166455; hereafter "Feigelson").*

Applicant traverses the rejection, and respectfully requests that the rejection be reconsidered and withdrawn.

As discussed regarding the rejection under 35 U.S.C. § 102, Rosen fails to teach or suggest all of the features of **Claim 1**. Further, Feigelson fails to compensate for the above deficiencies of Rosen, with respect to independent **Claim 1**, and nor was Feigelson cited for such purpose. Therefore, Applicant submits that **Claim 1** is patentable over the proposed combination of Rosen and Feigelson.

For at least the same reasons that **Claim 1** is patentable over Rosen and Feigelson, it is respectfully submitted that independent **Claims 12 and 24** are also patentable, to the extent that **Claims 12 and 24** recite similar features as **Claim 1.**

Further, while allegedly rejection **Claim 14** as being obvious over the combination of Rosen and Feigelson, the Office Action does not address **Claim 14** in the manner required by the MPEP. Specifically, the Office Action does not set forth grounds why the rejection regarding **Claim 14** has been made. For example, it appears that the Office Action does not consider "the second computer processor is further

configured to: read the inchoate disbursement transaction; compute a second cryptographic signature from the second private key; create a complete disbursement transaction record comprising: the commit input; the disbursement output; the first cryptographic signature; and the second cryptographic signature; and create a disbursement transaction by submitting the complete disbursement transaction record to the transfer mechanism," as recited in **Claim 14**. Accordingly, Applicant respectfully submits that a *prime facie* case of obviousness has not been established with regard to **Claim 14**, which is patentable over the purported combination of Rosen and Feigelson.

Claims 2, 13-23 and 25-30, variously depend, directly or indirectly, from independent **Claims 1, 12 and 24**, respectively. Therefore, Applicant submits that **Claims 2, 13-23 and 25-30** are patentable over the proposed combination of references at least by virtue of their dependency, as well as the other features recited therein. Applicant, therefore respectfully requests the reconsideration and withdrawal of rejection under 35 U.S.C. § 103.

CONCLUSION

It is respectfully submitted that other references in the record do not compensate for the deficiencies of the references utilized in rejecting the pending claims.

It should also be noted that although arguments have been presented with respect to certain claims herein, the recited subject matter as well as various other subject matter and/or combinations of subject matter may be patentable for other reasons. Further, the failure to address any statement by the Examiner herein should not be interpreted as acquiescence or agreement with such statement. Applicant expressly reserves the right to set forth additional and/or alternative reasons for patentability and/or allowance with the present Application or in any other future proceeding, and to rebut any statement presented by the Examiner in this or other papers during prosecution of the present Application.

All objections and rejections having been addressed, it is respectfully submitted that the present application is in condition for allowance, and therefore early and forthright issuance of a Notice to that effect is earnestly solicited.

Respectfully submitted,

Brundidge & Stanger, PC

Dated: October 24, 2019

/Misung Lee/
Misung Lee
Reg. No. 78,307

Notice of References Cited	Application/Control No. 15/309,612	Applicant(s)/Patent Under Reexamination Middleton et al.	
	Examiner JAMES D NIGH	Art Unit 3685	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-20130166455-A1	06-2013	Feigelson; Douglas	H04L9/3234	705/64
*	B	US-20030070080-A1	04-2003	Rosen, Sholom S.	G06Q20/02	713/187
	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	
	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.

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.
15/309,612	11/08/2016	Reginald Middleton	4675.1002BS	2321

86636 7590 12/11/2019

BRUNDIDGE & STANGER, P.C.
1925 BALLENGER AVENUE, STE. 560
ALEXANDRIA, VA 22314

EXAMINER	
NIGH, JAMES D	

ART UNIT	PAPER NUMBER
3685	

MAIL DATE	DELIVERY MODE
12/11/2019	PAPER

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.

Office Action Summary	Application No. 15/309,612	Applicant(s) Middleton et al.	
	Examiner JAMES D NIGH	Art Unit 3685	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 24 October 2019.

☐ 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) 1-30 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) 1-30 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: _____.

DETAILED ACTION

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.

Claim Status

2. As of the Office Action dated July 24, 2019 claims 1-30 were pending and claims 1-30 stood rejected. Claims 1, 3-5 and 7-30 have been amended. No claims have been added or cancelled. Claims 1-30 are therefore currently pending and are presented for examination on the merits.

Response to Arguments

3. Applicant's argument with regard to the 35 U.S.C. § 112 (b) or 35 U.S.C. § 112 (pre-AIA) 2nd paragraph rejection of claims 13, 27 and 30 has been fully considered but is not persuasive. As an initial matter paragraph 0055 says nothing regarding the combination of structure in the manner that is being claimed and only describes movement of function in the form of a client data store being embedded in a facilitator. Clearly this is not the same as claiming a first computer processor and the second computer processor are the same processor. Therefore the rejection has not been overcome and will be maintained.

4. Applicant's argument with regard to the 35 U.S.C. § 112 (d) or 35 U.S.C. § 112 (pre-AIA) 4th paragraph rejection of claims 13, 27 and 30 has been fully considered but is not persuasive. As an initial matter paragraph 0055 says nothing regarding the combination of structure in the manner that is being claimed and only describes movement of function in the form of a client data store being embedded in a facilitator.

Clearly this is not the same as claiming a first computer processor and the second computer processor are the same processor. Therefore the rejection has not been overcome and will be maintained.

5. Applicant's argument with regard to the 35 U.S.C. § 102 (a)(1) and (a)(2) rejection of claims 1 and 3-11 as being anticipated by Rosen (U.S. Patent Publication 2003/0070080) has been fully considered but is not persuasive. The Transaction Log Manager 36 as taught in paragraph 0162 as part of a transaction money module 4 (0157) which also contains a public key cryptography section (0189-0190). Therefore Applicant's argument that "…Rogen [sp] fails to teach or suggest the device comprising… 'a first memory comprising a transaction record section and a first key pair sector'" (pages 24 and 25 of argument) is clearly lacking in merit.

Applicant then argues at pages 25-28 that Rosen does not teach an inchoate transaction. The word "inchoate" per the Merriam-Webster dictionary means "being only partly in existence or operation" and must be viewed as a relative term with no clearly defined boundary as it pertains to a financial transaction as evidence that a transaction has been finalized only takes place once a recipient actually uses the funds in a transaction which is clearly not happening via the clearing and settlement processes being disclosed by Rosen. The written disclosure provides no definition of when a transaction is "inchoate" and aside from the use of the term as a modifier for the word transaction merely describes a clearing and settlement process and contextually only describes the term as a path towards transaction completion such as at page 16 "...8. The first client signs (i.e., computes a cryptographic signature and associates it with) a first principal input of an inchoate commit transaction record *for creating a*

complete commit transaction record", page 18 "...11. *The second client creates the complete commit transaction record by signing the inchoate commit transaction record*". Clearly the written disclosure itself uses the terms "inchoate" and "complete" in a manner that only suggests that a transaction is partially completed until an operation is performed that "completes" the transaction and therefore the written description is evidence that Examiner has appropriately applied the prior art against the claim. Clearly Applicant has failed to meet the necessary burden to establish clear error on the part of the Examiner. Therefore the present rejection of claim 1 will be maintained.

6. Applicant's argument with regard to the 35 U.S.C. § 102 (a)(1) and (a)(2) rejection of claims 3-11 as being anticipated by Rosen has been fully considered but is not persuasive. As the argument relies on the alleged deficiencies of Rosen as applied to claim 1 the argument is equally unpersuasive.

7. Applicant's argument with regard to the 35 U.S.C. § 103 rejection of claims 2 and 12-30 as being unpatentable over Rosen in view of Feigelson (U.S. Patent Publication 2013/0166455) has been fully considered but is not persuasive. As the argument relies on the alleged deficiencies of Rosen as applied to claim 1 the argument is equally unpersuasive.

Claim Rejections - 35 USC § 112

8. The following is a quotation of the first paragraph of 35 U.S.C. 112(a):

> (a) IN GENERAL.—The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor or joint inventor of carrying out the invention.

The following is a quotation of the first paragraph of pre-AIA 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor of carrying out his invention.

9. Claims 13, 27 and 30 are rejected under 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor or a joint inventor, or for pre-AIA the inventor(s), at the time the application was filed, had possession of the claimed invention.

10. Claim 13 recites "the first computer processor and the second computer processor are the same processor; the first memory and the second memory are the same memory; and the first network interface and the second network interface are the same network interface". Claims 27 and 30 contain similar recitations. Applicant indicated that support could be found at paragraph 0055. However in reviewing this paragraph the only teaching is that part or all of a client's data store may be embedded in the facilitator which is clearly not commensurate in scope with a claim claiming that two separate processors, memory and network interfaces are the same as is being claimed in claims 13, 27 and 30. Therefore the recitation is directed towards newly introduced subject matter.

11. 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.

12. Claims 13, 27 and 30 are 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.

13. Claim 13 recites "the first computer processor and the second computer processor are the same processor; the first memory and the second memory are the same memory; and the first network interface and the second network interface are the same network interface". Claims 27 and 30 contain similar recitations. It is unclear how two processors or memories can be "the same" and still be considered as separate structure, particularly when they have been assigned to separate pieces of structure "An essential purpose of patent examination is to fashion claims that are precise, clear, correct, and unambiguous. Only in this way can uncertainties of claim scope be removed…", In re Zletz,13 USPQ2d 1320 (Fed. Cir. 1989)

14. The following is a quotation of 35 U.S.C. 112(d):

> (d) REFERENCE IN DEPENDENT FORMS.—Subject to subsection (e), a claim in dependent form shall contain a reference to a claim previously set forth and then specify a further limitation of the subject matter claimed. A claim in dependent form shall be construed to incorporate by reference all the limitations of the claim to which it refers.

The following is a quotation of pre-AIA 35 U.S.C. 112, fourth paragraph:

> Subject to the following paragraph [i.e., the fifth paragraph of pre-AIA 35 U.S.C. 112], a claim in dependent form shall contain a reference to a claim previously set forth and then specify a further limitation of the subject matter claimed. A claim in dependent form shall be construed to incorporate by reference all the limitations of the claim to which it refers.

15. Claims 13, 27 and 30 are rejected under 35 U.S.C. 112(d) or pre-AIA 35 U.S.C. 112, 4th paragraph, as being of improper dependent form for failing to

further limit the subject matter of the claim upon which it depends, or for failing to include all the limitations of the claim upon which it depends.

16. Claim 13 recites "the first computer processor and the second computer processor are the same processor; the first memory and the second memory are the same memory; and the first network interface and the second network interface are the same network interface". Claims 27 and 30 contain similar recitations. As these were claimed as separate units of structure in claim 12 by saying that the "first... and the second… are the same" in claim 13 the claim is removing a limitation of claim 12 and thus is rejected under paragraph d of section 112. Similar reasoning applies to claims 27 and 30.

Claim Rejections - 35 USC § 102

17. 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.

18. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a)(1) the claimed invention was patented, described in a printed publication, or in public use, on sale or otherwise available to the public before the effective filing date of the claimed invention.
>
> (a)(2) the claimed invention was described in a patent issued under section 151, or in an application for patent published or deemed published under section 122(b), in which the patent or application, as the case may be, names another inventor and was effectively filed before the effective filing date of the claimed invention.

19. Claims 1 and 3-11 are rejected under 35 U.S.C. 102(a)(1) and (a)(2) as being anticipated by Rosen (U.S. Patent Publication 2003/0070080).

20. As per claim 1

Rosen discloses a device for facilitating a value transfer between a first party utilizing a first client and a second party utilizing a second client via a transfer mechanism (0026, 0149-0151, 0161 "The Pay/Exchange application 35 supervises the sending and receiving of electronic notes 11 between Transaction money modules 4", Figure 56)

Rosen discloses a first memory comprising a transaction record sector and a first key pair sector for storing a first asymmetric key pair, the first asymmetric key pair comprising a first private key and a first public key (0162 "The Tran Log Mgr. application 36 provides the management and overseeing of a log that records completed transactions undertaken by the money module", 0189-0190, 0685-0688 "Each primary trusted server 210 has its own public key and corresponding private key", claim 1, claim 2, claim 13)

Rosen discloses a first network interface for receiving terms (0231-0234)

Rosen discloses the terms comprising a first principal amount (0165)

Rosen discloses a reference to a first data source (0159, 1297)

Rosen discloses a first computer processor coupled to the first memory and the first network interface, the first computer processor configured to: retrieve a value from the first data source (0149, 0677)

Rosen discloses read the first private key from the first key pair sector (0504, claim 13)

Rosen discloses compute a first cryptographic signature from the first private key (0660, 0662, 0702)

Rosen discloses create an inchoate disbursement transaction record comprising: a commit input for receiving a commit amount from a commit transaction (0157, 0546, 1941)

Rosen discloses the first cryptographic signature (1946)

Rosen discloses publish the inchoate disbursement transaction record to at least one of the first client and the second client (0142-0143, 0588-0591, Figure 3, Figure 7, Figure 36A)

Rosen discloses where the first client comprises: a second memory comprising a second key pair sector for storing a second asymmetric key pair, the second asymmetric key pair comprising a second private key and a second public key (0142-0143, 0159, 0191, 0662, 0749, claim 91)

Rosen discloses a second network interface (0666)

Rosen discloses a second computer processor coupled to the second memory and the second network interface, the second computer processor configured to read the second private key from the second key pair sector (0630, 0664, 0749, Figure 52)

Rosen discloses where the second client comprises a third memory comprising a third key pair sector for storing a third asymmetric key pair, the third asymmetric key pair comprising a third private key and a third public key (1660-1663, Figure 57A)

Rosen discloses a third network interface (0670)

Rosen discloses a third computer processor coupled to the third memory and the third network interface, the third computer processor configured to read the third private key from the third key pair sector (0664, 1660-1663, Figure 56)

21. As per claim 3

Rosen discloses where: the first computer processor is further configured to compute a disbursement amount by applying a disbursement function to: the first principal amount; and the value from the first data source: and the inchoate disbursement transaction record further comprises a disbursement output comprising the disbursement amount (0157-0174)

22. As per claim 4

Rosen discloses where the first computer processor is further configured to: compute a second cryptographic signature from the first private key; create an inchoate refund transaction record comprising: a commit input for receiving the commit amount from the commit transaction: a refund output comprising a refund amount; the second cryptographic signature; and a lock time; and publish the inchoate refund transaction record to at least one of the first client or the second client (0157-0174, 0176-0179, 0251, 0300, 0806-0807, 0845)

23. As per claim 5

Rosen discloses where: the first key pair sector further stores a fourth asymmetric key pair, the fourth asymmetric key pair comprising a fourth private key and a fourth public key; and the first computer processor is further configured to: read the fourth private key from the first key pair sector; compute a second cryptographic signature from the fourth private key; create a commit transaction record, the commit

transaction record comprising: a first principal input for receiving the first principal amount from a first principal transaction; a commit output comprising the commit amount; the second cryptographic signature; and create the commit transaction by submitting the commit transaction record to the transfer mechanism (0177, 0193, 0546, 0662, 0791-0802, claims 1, 2 and 13)

24. As per claim 6

Rosen discloses where the first asymmetric key pair consists of the fourth asymmetric key pair, the first private key consists of the fourth private key, and the first public key consists of the fourth public key (0193, 0683-0688, 0854, Figure 56, claim 13)

25. As per claim 7

Rosen discloses where: the terms further comprises a second principal amount; and an expiration timestamp; the first computer processor is further configured to compute the one or more disbursement amounts by applying a disbursement function to: the value from the first data source; and at least one of: the first principal amount; and the second principal amount; and the inchoate disbursement transaction record further comprises one or more disbursement outputs comprising the disbursement amounts (0157-0174, 0176-0179, 0184, 0535, 0798-0802).

26. As per claim 8

Rosen discloses where: the terms further comprise: a reference to a second data source; the first computer processor is further configured to compute the one or more disbursement amounts by applying the disbursement function to: the value from the first

data source; the value from the second data source; the first principal amount; and the second principal amount (0157-0174, 0176-0179, 0184, 0279, 0284).

27. As per claim 9

Rosen discloses where: the reference to the first data source comprises at least one of a reference to a base instrument and a reference to a quote instrument; and the first computer processor is further configured to compute the disbursement amounts on or after the expiration timestamp (0118, 0180, 0278, 0284, 0535-0540, 0628)

28. As per claim 10

Rosen discloses where the first computer processor is further configured to: compute a second cryptographic signature from the first private key; create an inchoate refund transaction record comprising: a commit input for receiving the commit amount from the commit transaction; one or more refund outputs comprising one or more refund amounts; the second cryptographic signature; and a lock time; and publish the inchoate refund transaction record to at least one of the first client and the second client (0157-0174, 0176-0179, 0251, 0300, 0806-0807, 0845)

29. As per claim 11

Rosen discloses where: the first key pair sector further stores a fourth asymmetric key pair, the fourth asymmetric key pair comprising a fourth private key and a fourth public key; and the first computer processor is further configured to: read the fourth private key from the first key pair sector; compute a second cryptographic signature from the fourth private key; create a commit transaction record comprising: a first principal input for receiving the first principal amount from a first principal transaction; a second principal input for receiving the second principal amount from a

second principal transaction; a commit output comprising a commit amount; and the second cryptographic signature; and create the commit transaction by submitting the commit transaction record to the transfer mechanism (0177, 0193, 0255-0267, 0546, 0662, 0791-0802, 1723, claims 1, 2 and 13).

Claim Rejections - 35 USC § 103

30. 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.

31. Claim 2 is rejected under 35 U.S.C. 103 as being unpatentable over Rosen as applied to claim 1 above, and further in view of Feigelson (U.S. Patent Publication 2013/0166455).

32. As per claim 2

Rosen, while disclosing electronic money (Abstract), does not explicitly disclose wherein the transfer mechanism comprises a decentralized currency. Feigelson teaches wherein the transfer mechanism comprises a decentralized currency (0050-0051)

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the electronic monetary system of Rosen with the creation and use of digital currency of Feigelson for the purpose of maintaining secrecy of information in order to control its value (0003).

33. Claims 12-30 are rejected under 35 U.S.C. 103 as being unpatentable over Rosen and in view of Feigelson.

34. As per claim 12

Rosen discloses a device for facilitating a value transfer between a first party utilizing a first client and a second party utilizing a second client via a transfer mechanism (0026, 0149-0151, 0161 "The Pay/Exchange application 35 supervises the sending and receiving of electronic notes 11 between Transaction money modules 4", Figure 56)

Rosen discloses a first memory comprising a transaction record sector and a first key pair sector for storing a first asymmetric key pair, the first asymmetric key pair comprising a first private key and a first public key (0162 "The Tran Log Mgr. application 36 provides the management and overseeing of a log that records completed transactions undertaken by the money module", 0189-0190, 0685-0688 "Each primary trusted server 210 has its own public key and corresponding private key", claim 1, claim 2, claim 13)

Rosen discloses a first network interface for receiving terms (0231-0234)

Rosen discloses the terms comprising a first principal amount (0165)

Rosen discloses a reference to a first data source (0159, 1297)

Rosen discloses a first computer processor coupled to the first memory and the first network interface, the first computer processor configured to: retrieve a value from the first data source (0149, 0677)

Rosen discloses read the first private key from the first key pair sector (0504, claim 13)

Rosen discloses compute a first cryptographic signature from the first private key (0660, 0662, 0702)

Rosen discloses create an inchoate disbursement transaction record comprising: a commit input for receiving a commit amount from a commit transaction (0157, 0546, 1941)

Rosen discloses the first cryptographic signature (1946)

Rosen discloses publish the inchoate disbursement transaction record to at least one of the first client and the second client (0142-0143, 0588-0591, Figure 3, Figure 7, Figure 36A)

Rosen discloses where the first client comprises: a second memory comprising a second key pair sector for storing a second asymmetric key pair, the second asymmetric key pair comprising a second private key and a second public key (0142-0143, 0159, 0191, 0662, 0749, claim 91)

Rosen discloses a second network interface (0666)

Rosen discloses a second computer processor coupled to the second memory and the second network interface, the second computer processor configured to read the second private key from the second key pair sector (0630, 0664, 0749, Figure 52)

Rosen discloses where the second client comprises a third memory comprising a third key pair sector for storing a third asymmetric key pair, the third asymmetric key pair comprising a third private key and a third public key (1660-1663, Figure 57A)

Rosen discloses a third network interface (0670)

Rosen discloses a third computer processor coupled to the third memory and the third network interface, the third computer processor configured to read the third private key from the third key pair sector (0664, 1660-1663, Figure 56)

Rosen, while disclosing electronic money (Abstract), does not explicitly disclose wherein the transfer mechanism comprises a decentralized currency. Feigelson teaches wherein the transfer mechanism comprises a decentralized currency (0050-0051)

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the electronic monetary system of Rosen with the creation and use of digital currency of Feigelson for the purpose of maintaining secrecy of information in order to control its value (0003).

35. As per claim 13

Rosen discloses where: the facilitator and the client are the same device; the first computer processor and the second computer processor are the same processor; the first memory and the second memory are the same memory; and the first network interface and the second network interface are the same network interface (0143, 0147, 0157)

36. As per claims 14 and 25

Rosen discloses where: the first computer processor is further configured to compute a disbursement amount by applying a disbursement function to: the first principal amount; and the value from the first data source: and the inchoate disbursement transaction record further comprises a disbursement output comprising

the disbursement amount (0157-0174, 0177, 0193, 0288, 0504, 0546, 0662, 0791-0802, claims 1, 2 and 13)

37. As per claim 15

Rosen discloses where the first computer processor is further configured to: compute a second cryptographic signature from the first private key; create an inchoate refund transaction record comprising: a commit input for receiving the commit amount from the commit transaction; a refund output comprising a refund amount; and iii. the second cryptographic signature; and publish the inchoate refund transaction record to at least one of the first client and the second client. (0176-0179, 0251, 0300, 0806-0807)

38. As per claim 16

Rosen discloses where: the first key pair sector further stores a fourth asymmetric key pair, the fourth asymmetric key pair comprising a fourth private key and a fourth public key; the first computer processor is further configured to: compute a disbursement amount by applying a disbursement function to: the first principal amount; and the value from the first data source; read the fourth private key from the first key pair sector; compute a second cryptographic signature from the fourth private key; iv. create a commit transaction record comprising: a first principal input for receiving the first principal amount from a first principal transaction; a commit output comprising the commit amount; and the second cryptographic signature; and create the commit transaction by submitting the commit transaction record to the transfer mechanism; and the inchoate disbursement transaction record further comprises a disbursement output comprising the disbursement amount (0157-0174, 0177, 0193, 0546, 0662, 0791-0802, claims 1, 2 and 13)

39. As per claim 17

Rosen discloses where the second computer processor is configured to: compute a third cryptographic signature from the second private key; create a first principal transaction record comprising: a first principal output comprising the first principal amount; and the third cryptographic signature; and create the first principal transaction by submitting the first principal transaction record to the transfer mechanism (0157-0174, 0176-0179, 0300, 0791-0802)

40. As per claim 18

Rosen discloses where: a. the terms further comprise: a second principal amount; and ii. an expiration timestamp; the first computer processor is further configured compute one or more disbursement amounts by applying a disbursement function to: the value from the first data source; and at least one of: the first principal amount; and the second principal amount; the inchoate disbursement transaction record further comprises one or more disbursement outputs comprising the disbursement amounts; and the second computer processor is further configured to: read the inchoate disbursement transaction; compute a second cryptographic signature from the second private key; create a complete disbursement transaction record comprising : the commit input; the disbursement outputs; the first cryptographic signature; and the second cryptographic signature; and create a disbursement transaction by submitting the complete disbursement transaction record to the transfer mechanism (0157-0174, 0176-0179, 0288, 0504, 0535, 0546, 0791-0802)

41. As per claim 19

Rosen discloses where: the terms further comprise: a reference to a second data source; the first computer processor is further configured to compute the one or more disbursement amounts by applying the disbursement function to: the value from the first data source; the value from the second data source; the first principal amount; and the second principal amount (0157-0174, 0176-0179, 0184, 0279, 0284)

42. As per claim 20

Rosen discloses where: the reference to the first data source comprises at least one of a reference to a base instrument and a reference to a quote instrument; and the first computer processor is further configured to compute the disbursement amounts on or after the expiration timestamp (0118, 0180, 0278, 0284, 0535-0540, 0628)

43. As per claim 21

Rosen discloses where: a. the terms further comprise: a second principal amount; and ii. an expiration timestamp; the first computer processor is further configured to: compute one or more disbursement amounts by applying a disbursement function to: the value from the first data source; and at least one of: the first principal amount; and the second principal amount; compute a second cryptographic signature from the first private key; create an inchoate refund transaction record comprising: a commit input for receiving the commit amount from the commit transaction: a refund output comprising a refund amount; and the second cryptographic signature; and publish the inchoate refund transaction record to at least one of the first client and the second client; and the inchoate disbursement transaction record further comprises one or more disbursement outputs comprising the disbursement amounts (0157-0174, 0176-0179, 0251, 0300, 0535, 0791-0802, 0806-0807, 0845)

44. As per claim 22

Rosen discloses where: the terms further comprise: a second principal amount; and ii. an expiration timestamp; the first key pair sector further stores a fourth asymmetric key pair, the fourth asymmetric key pair comprising a fourth private key and a fourth public key; the first computer processor is further configured to: compute one or more disbursement amounts by applying a disbursement function to: the value from the first data source; and at least one of: the first principal amount; and the second principal amount; read the fourth private key from the first key pair sector; compute a second cryptographic signature from the fourth private key; create a commit transaction record comprising: a first principal input for receiving the first principal amount from the first principal transaction; a second principal input for receiving the second principal amount from the second principal transaction; a commit output comprising the commit amount; and the second cryptographic signature; and create the commit transaction by submitting the commit transaction record to the transfer mechanism; and the inchoate disbursement transaction record further comprises one or more disbursement outputs comprising the disbursement amounts (0157-0174, 0176-0179, 0251, 0300, 0535, 0791-0802, 0806-0807).

45. As per claim 23

Rosen discloses where: the second computer processor is further configured to: compute a third cryptographic signature from the second private key; create a first principal transaction record comprising: a first principal output comprising the first principal amount; and the third cryptographic signature; and create a first principal transaction by submitting the first principal transaction record to the transfer

mechanism; and the third computer processor is further configured to: compute a fourth cryptographic signature from the third private key; create a second principal transaction record comprising: a second principal output comprising the second principal amount; and the fourth cryptographic signature; and create a second principal transaction by submitting the second principal transaction record to the transfer mechanism (0157-0174, 0176-0179, 0300, 0490, 0662, 0791-0802)

46. As per claim 24

Rosen discloses a method for facilitating value transfers via a transfer mechanism (0149-0151, 0161, Figure 56)

Rosen discloses the transfer mechanism comprising a digital currency (0118)

Rosen discloses the method comprising: storing a first asymmetric key pair in a first key pair sector of a first memory, the first asymmetric key pair comprising a first private key and a first public key (0162, 0189-0190, 0685-688, claims 1, 2 and 13)

Rosen discloses storing a second asymmetric key pair in a second key pair sector of a second memory, the second asymmetric key pair comprising a second private key and a second public key (0142-0143, 0159, 0749, claim 91)

Rosen discloses storing a third asymmetric key pair in the second key pair sector, the third key pair comprising a third private key and a third public key (1660-1663, Figure 57A)

Rosen discloses storing a fourth asymmetric key pair in a third key pair sector of a third memory, the fourth asymmetric key pair comprising a fourth private key and a fourth public key (0193, 0683-0688, 0854, Figure 56, claim 13)

Rosen discloses transmitting terms from a client via a first network interface (0231-0234) the terms comprising: a first principal amount (0165) and a reference to a first data source (0159, 1297)

Rosen discloses receiving the terms at a facilitator via a second network interface (0026, 0589, 0666)

Rosen discloses reading the first private key from the first key pair sector (0504, claim 13)

Rosen discloses computing a first cryptographic signature from the first private key (0660, 0662, 0702)

Rosen discloses creating a first principal transaction record comprising: a first principal output comprising the first principal amount; and the first cryptographic signature (0157-0174)

Rosen discloses creating a first principal transaction by submitting the first principal transaction record to the transfer mechanism (0546, 0791-0802)

Rosen discloses reading the second private key from the second key pair sector (0630, 0664, 0749, Figure 52)

Rosen discloses computing a second cryptographic signature from the second private key (0660, 0662)

Rosen discloses creating a commit transaction record comprising: a first principal input for receiving the first principal amount from the first principal transaction; a commit output comprising a commit amount; and iii. the second cryptographic signature (0157-0174, 0176-0179, 0300, 0535, 0791-0802)

Rosen discloses creating the commit transaction by submitting the commit transaction record to the transfer mechanism (0157-0174, 0176-0179, 0300, 0535, 0791-0802)

Rosen discloses retrieving a value from the first data source (0149, 0677)

Rosen discloses reading the third private key from the second key pair sector (0664, 1660-1663, Figure 56)

Rosen discloses computing a third cryptographic signature from the second private key (0157-0174, 0176-0179, 0193, 0300, 0791-0802)

Rosen discloses creating an inchoate disbursement transaction record comprising: a commit input for receiving a commit amount from a commit transaction; the third cryptographic signature (0157-0174, 0176-0179, 0193, 0300, 0791-0802)

Rosen discloses publishing the inchoate disbursement transaction record (0157-0174, 0176-0179, 0193, 0300, 0791-0802)

Rosen discloses reading the inchoate disbursement transaction record (0157-0174, 0176-0179, 0193, 0300, 0660, 0662, 0791-0802)

Rosen discloses reading the fourth private key from the third key pair sector (0157-0174, 0176-0179, 0193, 0300, 0660, 0662, 0791-0802)

Rosen discloses computing a fourth cryptographic signature from the fourth private key (0157-0174, 0176-0179, 0193, 0300, 0660, 0662, 0791-0802)

Rosen discloses creating a complete disbursement transaction record comprising: the commit input; the third cryptographic signature; and the fourth cryptographic signature (0157-0174, 0176-0179, 0193, 0300, 0660, 0662, 0791-0802)

Rosen discloses creating a disbursement transaction by submitting the complete disbursement transaction record to the transfer mechanism (0157-0174, 0176-0179, 0193, 0300, 0660, 0662, 0791-0802)

Rosen, while disclosing electronic money (Abstract), does not explicitly disclose wherein the transfer mechanism comprises a decentralized currency. Feigelson teaches wherein the transfer mechanism comprises a decentralized currency (0050-0051)

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the electronic monetary system of Rosen with the creation and use of digital currency of Feigelson for the purpose of maintaining secrecy of information in order to control its value (0003).

47. As per claim 25

Rosen discloses a. computing a disbursement amount by applying a disbursement function to: the first principal amount; and the value from the first data source; and where: the inchoate disbursement transaction record further comprises a disbursement output comprising the disbursement amount; and the complete disbursement transaction record further comprises the disbursement output (0157-0174, 0791-0802)

48. As per claim 26

Rosen discloses computing a fifth cryptographic signature from the third private key; creating an inchoate refund transaction record comprising: a commit input for receiving the commit amount from the commit transaction; a refund output comprising a refund amount; the fifth cryptographic signature; and a lock time; and publishing the

inchoate refund transaction record (0157-0174, 0176-0179, 0251, 0300, 0660, 0662, 0806-0807, 0845)

49. As per claim 27

Rosen discloses where at least one of: the second asymmetric key pair consists of the third asymmetric key pair, the second private key consists of the third private key, and the second public key consists of the third public key; the first asymmetric key pair consists of the fourth asymmetric key pair, the first private key consists of the fourth private key, and the first public key consists of the fourth public key; and the first memory and the third memory are the same memory and the first key pair sector consists of the third key pair sector (claims 1, 2 and 13)

50. As per claim 28

Rosen discloses storing a fifth asymmetric key pair in a fourth key pair sector of a fourth memory, the fifth asymmetric key pair comprising a fifth private key and a fifth public key; reading the fifth private key from the fourth key pair sector; computing a fifth cryptographic signature from the fifth private key; creating a second principal transaction record comprising: a second principal output comprising the second principal amount; and the fifth cryptographic signature; creating a second principal transaction by submitting the second principal transaction record to the transfer mechanism; computing one or more disbursement amounts by applying a disbursement function to: the value from the first data source; and at least one of: the first principal amount; and the second principal amount; and where: the inchoate disbursement transaction record further comprises one or more disbursement outputs comprising the disbursement

amounts; and the complete disbursement transaction record further comprises the disbursement outputs (0157-0174, 0176-0179, 0288, 0504, 0535, 0546, 0791-0802)

51. As per claim 29

Rosen discloses computing a sixth cryptographic signature from the third private key; creating an inchoate refund transaction record comprising: a commit input for receiving the commit amount from the commit transaction; one or more refund outputs comprising one or more refund amounts; the sixth cryptographic signature; and a lock time; and publishing the inchoate refund transaction record (0157-0174, 0176-0179, 0251, 0300, 0660, 0662, 0806-0807, 0845)

52. As per claim 30

Rosen discloses where at least one of: the second asymmetric key pair consists of the third asymmetric key pair, the second private key consists of the third private key, and the second public key consists of the third public key; the first asymmetric key pair consists of the fourth asymmetric key pair, the first private key consists of the fourth private key, and the first public key consists of the fourth public key; the fifth asymmetric key pair consists of the fourth asymmetric key pair, the fifth private key consists of the fourth private key, and the fifth public key consists of the fourth public key; the first memory and the third memory are the same memory and the first key pair sector consists of the third key pair sector; and the fourth memory and the third memory are the same memory and the fifth key pair sector consists of the third key pair sector (claim 1, claim 2 and claim 13).

Conclusion

53. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

54. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JAMES D NIGH whose telephone number is (571)270-5486. The examiner can normally be reached on 6-9 AM and 11 AM TO 4 PM.

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, Neha Patel can be reached on (571) 270-1492. 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.

/JAMES D NIGH/
Primary Examiner, Art Unit 3685

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/309,612	Middleton et al.
	Examiner	Art Unit
	JAMES D NIGH	3685

CPC - Searched*		
Symbol	Date	Examiner

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
EAST Text Search	07/18/2019	JDN

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

	/JAMES D NIGH/ Primary Examiner, Art Unit 3685

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	5	("20030070080" | "20130054471" | "20130166455" | "20130179337" | "20130212388").PN.	US-PGPUB; USPAT	AND	ON	2019/07/18 07:53
S2	17	(server near20 ("public key") near20 ("private key")) ((transaction or principal) near10 amount) (signature near20 "private key") ((client or agent) near20 "private key") ((digital or electronic) near10 currency) @ad<="20140509"	US-PGPUB; USPAT	AND	ON	2019/07/18 08:22
S3	2	("20170187535").PN.	US-PGPUB; USPAT; USOCR; DERWENT	AND	ON	2019/12/09 12:05

12/10/2019 6:02:56 AM
C:\Users\jnigh\Documents\EAST\Workspaces\15309612.wsp

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application Serial No..... 15/309,612
Filing Date ..... November 08, 2016
Confirmation No. 2321
Inventorship ..... Reginald Middleton
Group Art Unit..... 3685
Examiner .....NIGH, JAMES D
Attorney Docket No. 4675.1002BS
Title: .....Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers

RESPONSE TO FINAL OFFICE ACTION OF DECEMBER 11, 2019 AND REQUEST FOR CONTINUED EXAMINATION UNDER 37 CFR 1.114

To: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

From: Misung Lee
Customer No. 86636
Brundidge & Stanger, PC
1925 Ballenger Ave., Suite 560
Alexandria, VA 22314

Sir:

In response to the Final Office Action dated December 11, 2019, for which the three-month shortened statutory period for response is set to expire on March 11, 2020, the following amendments and remarks are respectfully submitted with the concurrently filed Request for Continued Examination in compliance with 37 CFR § 1.114. Favorable consideration is respectfully requested.

The Commissioner is hereby authorized to charge any deficiency of fees and credit any overpayments to Deposit Account Number 50-4888.

INTRODUCTORY COMMENTS

The Listing of the Claims section begins on page 3.

Remarks section begins on page 18.

LISTING OF THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Claims pending:

- At time of the Action: **Claims 1-30**
- After this Reply: **Claims 1, 3-6, 9, 12, 15-17, 20, 23, 24, 26, 28, 29 and 31**

Currently Canceled or Withdrawn Claims: **Claims 2, 7, 8, 10, 11, 13, 14, 18, 19, 21, 22, 25, 27, and 30**

Currently Amended Claims: **Claims 1, 3, 4, 5, 9, 12, 15-17, 20, 23, 24, 26, and 28**

New Claims: **Claim 31**

1. (**Currently Amended**) A device for facilitating a value transfer between a first party utilizing a first client and a second party utilizing a second client via a transfer mechanism, the transfer mechanism comprising a decentralized digital currency, the device comprising:

a first memory comprising a transaction record sector and a first key pair sector for storing a first asymmetric key pair, the first asymmetric key pair comprising a first private key and a first public key;

a first network interface for receiving terms, the terms comprising:

at least one of a first principal amount or a second principal amount; ~~and~~

a reference to at least one of a first data source or a second data source; and

an expiration timestamp;

a first computer processor coupled to the first memory and the first network interface, the first computer processor configured to:

~~retrieve a value from the first data source;~~compute one or more disbursement amounts by applying a disbursement function to:

at least one of the first principal amount or the second principal amount, and

a value from at least one of the first data source or the second data source;

read the first private key from the first key pair sector;

compute a first cryptographic signature from the first private key;

create an inchoate disbursement transaction record comprising:

a commit input for receiving a commit amount from a commit transaction; ~~and~~

one or more disbursement outputs comprising the disbursement amounts; and

the first cryptographic signature; and

publish the inchoate disbursement transaction record to at least one of the first client and the second client;

where the first client comprises:

a second memory comprising a second key pair sector for storing a second asymmetric key pair, the second asymmetric key pair comprising a second private key and a second public key;

a second network interface; and

a second computer processor coupled to the second memory and the second network interface, the second computer processor configured to:

read the second private key from the second key pair sector; ~~and~~

read the inchoate disbursement transaction record;

compute a second cryptographic signature from the second private key;

create a complete disbursement transaction record comprising:

the commit input;

the disbursement outputs;

the first cryptographic signature; and

the second cryptographic signature; and

create a disbursement transaction by submitting the complete disbursement transaction record to the transfer mechanism; and

where the second client comprises;

a third memory comprising a third key pair sector for storing a third asymmetric key pair, the third asymmetric key pair comprising a third private key and a third public key;

a third network interface; and

a third computer processor coupled to the third memory and the third network interface, the third computer processor configured to read the third private key from the third key pair sector.

2. (**Canceled**)

3. (**Currently Amended**) The device of claim 1, where:

the first computer processor is ~~further~~ configured to compute ~~a~~ the one or more disbursement amounts by applying ~~a~~ the disbursement function to:

the first principal amount; and

[[.]] the value from the first data source~~; and~~

~~the inchoate disbursement transaction record further comprises a disbursement output comprising the disbursement amount~~.

4. (**Currently Amended**) The device of claim ~~3~~ 1, where the first computer processor is further configured to:

compute a ~~second~~ third cryptographic signature from the first private key;

create an inchoate refund transaction record comprising:

a commit input for receiving the commit amount from the commit transaction;

a refund output comprising a refund amount;

the ~~second~~ third cryptographic signature; and

a lock time; and

publish the inchoate refund transaction record to at least one of the first client or the second client.

5. (**Currently Amended**) The device of claim ~~3~~1, where:

the first key pair sector further stores a fourth asymmetric key pair, the fourth asymmetric key pair comprising a fourth private key and a fourth public key; and

the first computer processor is further configured to:

read the fourth private key from the first key pair sector;

compute a ~~second~~ third cryptographic signature from the fourth private key;

create a commit transaction record, the commit transaction record comprising:

a first principal input for receiving the first principal amount from a first principal transaction;

a commit output comprising the commit amount;

the ~~second~~ third cryptographic signature; and

create the commit transaction by submitting the commit transaction record to the transfer mechanism.

6. (**Original**) The device of claim 5, where the first asymmetric key pair consists of the fourth asymmetric key pair, the first private key consists of the fourth private key, and the first public key consists of the fourth public key.

7. (**Canceled**)

8. (**Canceled**)

9. (**Currently Amended**) The device of claim ~~7~~1, where:

the reference to the first data source comprises at least one of a reference to a base instrument and a reference to a quote instrument; and

the first computer processor is further configured to compute the disbursement amounts on or after the expiration timestamp.

10. (**Canceled**)

11. (**Canceled**)

12. (**Currently Amended**) A system for facilitating a value transfer between a first party utilizing a first client and a second party utilizing a second client via a transfer mechanism, the transfer mechanism comprising a decentralized digital currency, the system comprising a facilitator, the first client, and the second client;

the facilitator comprising:

a first memory comprising a transaction record sector and a first key pair sector for storing a first asymmetric key pair, the first asymmetric key pair comprising a first private key and a first public key;

a first network interface for receiving terms, the terms comprising:

at least one of a first principal amount or a second principal amount; ~~and~~

a reference to at least one of a first data source or a second data source; and

an expiration timestamp; and

a first computer processor coupled to the first memory and the first network interface, the first computer processor configured to:

compute one or more disbursement amounts by applying a disbursement function to:

at least one of the first principal amount or the second principal amount, and

a value from at least one of the first data source or the second data source;

~~retrieve a value from the first data source;~~

read the first private key from the first key pair sector;

compute a first cryptographic signature from the first private key;

create an inchoate disbursement transaction record comprising:

a commit input for receiving a commit amount from a commit transaction; ~~and~~

one or more disbursement outputs comprising the disbursement amounts; and

the first cryptographic signature; and

publish the inchoate disbursement transaction record to at least one of the first client and the second client;

the first client comprising:

a second memory comprising a second key pair sector for storing a second asymmetric key pair, the second asymmetric key pair comprising a second private key and a second public key;

a second network interface; and

a second computer processor coupled to the second memory and the second network interface, the second computer processor configured to:

read the second private key from the second key pair sector; ~~and~~

read the inchoate disbursement transaction record;

compute a second cryptographic signature from the second private key;

create a complete disbursement transaction record comprising:

the commit input;

the disbursement outputs;

the first cryptographic signature; and

the second cryptographic signature; and

create a disbursement transaction by submitting the complete disbursement transaction record to the transfer mechanism; and

the second client comprising:

a third memory comprising a third key pair sector for storing a third asymmetric key pair, the third asymmetric key pair comprising a third private key and a third public key;

a third network interface; and

a third computer processor coupled to the third memory and the third network interface, the third computer processor configured to read the third private key from the third key pair sector.

13. (**Canceled**)

14. (**Canceled**)

15. (**Currently Amended**) The system of claim 12, where the first computer processor is further configured to:

compute a ~~second~~ third cryptographic signature from the first private key;

create an inchoate refund transaction record comprising:

a commit input for receiving the commit amount from the commit transaction;

a refund output comprising a refund amount; and

the ~~second~~ third cryptographic signature; and

publish the inchoate refund transaction record to at least one of the first client and the second client.

16. (**Currently Amended**) The system of claim 12, where:

the first key pair sector further stores a fourth asymmetric key pair, the fourth asymmetric key pair comprising a fourth private key and a fourth public key;

the first computer processor is further configured to:

compute ~~a~~ the one or more disbursement amounts by applying ~~a~~ the disbursement function to:

the first principal amount; and

the value from the first data source;

read the fourth private key from the first key pair sector;

compute a ~~second~~ third cryptographic signature from the fourth private key;

create a commit transaction record comprising:

a first principal input for receiving the first principal amount from a first principal transaction;

a commit output comprising the commit amount; and

the ~~second~~ third cryptographic signature; and

create the commit transaction by submitting the commit transaction record to the transfer mechanism~~; and~~

~~the inchoate disbursement transaction record further comprises a disbursement output comprising the disbursement amount~~.

17. (**Currently Amended**) The system of claim 16, where the second computer processor is configured to:

compute a ~~third~~ fourth cryptographic signature from the second private key;

create a first principal transaction record comprising:

a first principal output comprising the first principal amount; and

the ~~third~~ fourth cryptographic signature; and

create the first principal transaction by submitting the first principal transaction record to the transfer mechanism.

18. (**Canceled**)

19. (**Canceled**)

20. (**Currently Amended**) The system of claim ~~18~~12, where:

the reference to at least one of the first data source or the second data source comprises at least one of a reference to a base instrument ~~and~~ or a reference to a quote instrument; and

the first computer processor is further configured to compute the disbursement amounts on or after the expiration timestamp.

21. (**Canceled**)

22. (**Canceled**)

23. (**Currently Amended**) The system of claim ~~22~~ 12, where:

the second computer processor is further configured to:

compute a third cryptographic signature from the second private key;

create a first principal transaction record comprising:

a first principal output comprising the first principal amount; and

the third cryptographic signature; and

create a first principal transaction by submitting the first principal transaction record to the transfer mechanism; and

the third computer processor is further configured to:

compute a fourth cryptographic signature from the third private key;

create a second principal transaction record comprising:

a second principal output comprising the second principal amount; and

the fourth cryptographic signature; and

create a second principal transaction by submitting the second principal transaction record to the transfer mechanism.

24. (**Currently Amended**) A method for facilitating value transfers between a first party utilizing a first client and a second party utilizing a second client via a transfer mechanism, the transfer mechanism comprising a decentralized digital currency, the method comprising:

storing a first asymmetric key pair in a first key pair sector of a first memory, the first asymmetric key pair comprising a first private key and a first public key;

storing a second asymmetric key pair in a second key pair sector of a second memory, the second asymmetric key pair comprising a second private key and a second public key;

storing a third asymmetric key pair in the second key pair sector, the third key pair comprising a third private key and a third public key;

storing a fourth asymmetric key pair in a third key pair sector of a third memory, the fourth asymmetric key pair comprising a fourth private key and a fourth public key;

transmitting terms from ~~a~~ one of the first or second client via a first network interface, the terms comprising:

at least one of a first principal amount or a second principal amount; ~~and~~

a reference to at least one of a first data source or a second data source; and

an expiration timestamp;

receiving the terms at a facilitator via a second network interface;

computing one or more disbursement amounts by applying a disbursement function to:

at least one of the first principal amount or the second principal amount, and

a value from at least one of the first data source or the second data source;

reading the first private key from the first key pair sector;

computing a first cryptographic signature from the first private key;

creating a first principal transaction record comprising:

a first principal output comprising the first principal amount; and

the first cryptographic signature;

creating a first principal transaction by submitting the first principal transaction record to the transfer mechanism;

reading the second private key from the second key pair sector;

computing a second cryptographic signature from the second private key;

creating a commit transaction record comprising:

a first principal input for receiving the first principal amount from the first principal transaction;

a commit output comprising a commit amount; and

the second cryptographic signature;

creating the commit transaction by submitting the commit transaction record to the transfer mechanism;

retrieving a value from the first data source;

reading the third private key from the second key pair sector;

computing a third cryptographic signature from the second private key;

creating an inchoate disbursement transaction record comprising:

a commit input for receiving a commit amount from a commit transaction;

one or more disbursement outputs comprising the one or more disbursement amounts; and

the third cryptographic signature;

publishing the inchoate disbursement transaction record;

reading the inchoate disbursement transaction record;

reading the fourth private key from the third key pair sector;

computing a fourth cryptographic signature from the fourth private key;

creating a complete disbursement transaction record comprising:

the commit input;

the one or more disbursement outputs;

the third cryptographic signature; and

the fourth cryptographic signature; and

creating a disbursement transaction by submitting the complete disbursement transaction record to the transfer mechanism.

25. (**Canceled**)

26. (**Currently Amended**) The method of claim ~~25~~24, further comprising:

computing a fifth cryptographic signature from the third private key;

creating an inchoate refund transaction record comprising:

a commit input for receiving the commit amount from the commit transaction;

a refund output comprising a refund amount;

the fifth cryptographic signature; and

a lock time; and

publishing the inchoate refund transaction record.

27. (**Canceled**)

28. (**Currently Amended**) The method of claim 24, further comprising:

storing a fifth asymmetric key pair in a fourth key pair sector of a fourth memory, the fifth asymmetric key pair comprising a fifth private key and a fifth public key;

reading the fifth private key from the fourth key pair sector;

computing a fifth cryptographic signature from the fifth private key;

creating a second principal transaction record comprising:

a second principal output comprising the second principal amount; and

the fifth cryptographic signature;

creating a second principal transaction by submitting the second principal transaction record to the transfer mechanism~~;~~

computing one or more disbursement amounts by applying a disbursement function to:

the value from the first data source; and at least one of:

the first principal amount; and

the second principal amount;~~ and~~

~~where:~~

~~the inchoate disbursement transaction record further comprises one or more disbursement outputs comprising the disbursement amounts; and~~

~~the complete disbursement transaction record further comprises the disbursement outputs~~.

29. (**Previously Presented**) The method of claim 28, further comprising:

computing a sixth cryptographic signature from the third private key;

creating an inchoate refund transaction record comprising:

a commit input for receiving the commit amount from the commit transaction;

one or more refund outputs comprising one or more refund amounts;

the sixth cryptographic signature; and

a lock time; and

publishing the inchoate refund transaction record.

30. (**Canceled**)

31. (**New**) The method of claim 24, wherein the one or more disbursement output further comprise one or more conditions requiring approval of at least one of the first party or the second party, and the one or more conditions include a condition to determine if a sum of the one or more disbursement amounts is equal or less than the commit amount from the commit transaction.

Electronic Acknowledgement Receipt

EFS ID:	38828960
Application Number:	15309612
International Application Number:	
Confirmation Number:	2321
Title of Invention:	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers
First Named Inventor/Applicant Name:	Reginald Middleton
Customer Number:	86636
Filer:	Misung Lee/Juel Clyne
Filer Authorized By:	Misung Lee
Attorney Docket Number:	4675.1002BS
Receipt Date:	11-MAR-2020
Filing Date:	08-NOV-2016
Time Stamp:	10:40:47
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	$650
RAM confirmation Number	E20203AA41034631
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	Response After Final Action	4675_FOA_Response.pdf	175329 2edfc620239ccf7a6e3617b3b608aa43429c2eab	no	26
Warnings:					
Information:					
2	Request for Continued Examination (RCE)	4675_20200311_RCE.pdf	1350130 3b55f2f9132c9e520052c6b133e83c4ff13b985f	no	3
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30654 577cd2035d0768dafaf0da6be0fa92dfd74ddbcc	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1556113		

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.

PTO/SB/30EFS (02-18)
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 contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	15/309,612	Filing Date	2016-11-08	Docket Number (if applicable)	4675.1002BS	Art Unit	3685
First Named Inventor	Reginald Middleton			Examiner Name	James D. Nigh		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

- ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
- ☐ Other _____

☒ Enclosed

- ☒ Amendment/Reply
- ☐ Information Disclosure Statement (IDS)
- ☐ Affidavit(s)/ Declaration(s)
- ☐ Other _____

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____ (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

☒ **The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 504888

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature

Applicant Signature

PTO/SB/30EFS (02-18)
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 contains a valid OMB control number.

Signature of Registered U.S. Patent Practitioner			
Signature	/Misung Lee/	Date (YYYY-MM-DD)	2020-03-11
Name	Misung Lee	Registration Number	78307

This collection of information is required by 37 CFR 1.114. 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.

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

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 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 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.

REMARKS

Reconsideration and allowance in view of the foregoing amendments and the following remarks are respectfully requested.

Claims 1-30 are pending. **Claims 13, 27, and 30** were rejected under 35 U.S.C. § 112(a)/(b)/(d). **Claims 1 and 3-11** were rejected under 35 U.S.C. § 102(a)(1)/(a)(2). **Claims 2 and 12-30** were rejected under 35 U.S.C. § 103. Upon entry of the amendment, **Claims 1, 3, 4, 5, 9, 12, 15-17, 20, 23, 24, 26, and 28** are currently amended and **Claims 2, 7, 8, 10, 11, 13, 14, 18, 19, 21, 22, 25, 27, and 30** are currently canceled. Support for the amendments to independent **Claims 1, 11, and 24** can be found, at least at, **Claims 2, 7, 8, 10, 11, 14, 18, 19, 21, 22, and 25,** which are currently canceled without prejudice or disclaimer. Support for new **Claim 31** can be found, at least at, paragraph [0131] of the U.S. Patent Application Publication. No new matter is added.

Favorable consideration is respectfully requested.

CLAIM REJECTION UNDER 35 U.S.C. § 112

Claims 13, 27, and 30 *are rejected under 35 U.S.C. § 112(a) or 35 U.S.C. § 112 (pre-AIA), first paragraph, as allegedly failing to comply with the written description requirement.*

Claims 13, 27, and 30 *are rejected under 35 U.S.C. § 112(b) or 35 U.S.C. § 112 (pre-AIA), second paragraph, as allegedly 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.*

Claims 13, 27, and 30 *are rejected under 35 U.S.C. § 112(d) or 35 U.S.C. § 112 (pre-AIA), fourth paragraph, as allegedly being of improper dependent form for failing to further limit the subject matter of the claim upon which it depends, or for failing to include all the limitations of the claim upon which it depends.*

Applicant traverses the rejections, and respectfully requests that the rejections be reconsidered and withdrawn. Nevertheless, without conceding the propriety of the rejections, but rather as a part of cooperative efforts to expedite the prosecution of this application to allowance, Applicant is currently canceling **Claims 13, 27, and 30**. Accordingly, the rejections to the claims are moot based on

cancellation of **Claims 13, 27, and 30**. Applicant, therefore respectfully requests the reconsideration and withdrawal of rejections.

CLAIM REJECTIONS

*a) **Claims 1 and 3-11** are rejected under 35 U.S.C. § 102(a)(1) and (a)(2) as allegedly being anticipated by Rosen (U.S. Publication No. 2003/0070080; hereafter "Rosen").*

*b) **Claim 2** is rejected under 35 U.S.C. § 103 as allegedly being unpatentable over Rosen and further in view of Feigelson (U.S. Publication No. 2013/0166455; hereafter "Feigelson").*

*c) **Claims 12-30** are rejected under 35 U.S.C. § 103 as allegedly being unpatentable over Rosen and in view of Feigelson.*

Applicant traverses the rejections, and respectfully requests that the rejections be reconsidered and withdrawn. Among independent **Claims 1, 11, and 24**, Applicant will discuss **Claim 24** as being representative, but only to the extent that similar features are recited in all three independent claims. Applicant submits that the scope and features of the independent claims are not identical.

Without conceding the propriety of the rejections, but rather as a part of cooperative efforts to expedite the prosecution of this application to allowance, Applicant is currently amending independent **Claim 24**. Currently amended **Claim 24** recites (emphasis added):

> A method for ***facilitating value transfers via a transfer mechanism, the transfer mechanism comprising a decentralized digital currency***, the method comprising:
>
> storing a first asymmetric key pair in a first key pair sector of a first memory, the first asymmetric key pair comprising a first private key and a first public key;
>
> storing a second asymmetric key pair in a second key pair sector of a second memory, the second asymmetric key pair comprising a second private key and a second public key;
>
> storing a third asymmetric key pair in the second key pair sector, the third key pair comprising a third private key and a third public key;
>
> storing a fourth asymmetric key pair in a third key pair sector of a third memory, the fourth asymmetric key pair comprising a fourth private key and a fourth public key;

transmitting terms from a client via a first network interface, the terms comprising:

at least one of a first principal amount or a second principal amount;

a reference to at least one of a first data source or a second data source; and

an expiration timestamp;

receiving the terms at a facilitator via a second network interface;

computing one or more disbursement amounts by applying a disbursement function to:

at least one of the first principal amount or the second principal amount, and

a value from at least one of the first data source or the second data source;

reading the first private key from the first key pair sector;

computing a first cryptographic signature from the first private key;

creating a first principal transaction record comprising:

a first principal output comprising the first principal amount; and

the first cryptographic signature;

creating a first principal transaction by submitting the first principal transaction record to the transfer mechanism;

reading the second private key from the second key pair sector;

computing a second cryptographic signature from the second private key;

creating a commit transaction record comprising:

a first principal input for receiving the first principal amount from the first principal transaction;

a commit output comprising a commit amount; and

the second cryptographic signature;

creating the commit transaction by submitting the commit transaction record to the transfer mechanism;

retrieving a value from the first data source;

reading the third private key from the second key pair sector;

computing a third cryptographic signature from the second private key;

creating an inchoate disbursement transaction record comprising:

a commit input for receiving a commit amount from a commit transaction;

one or more disbursement outputs comprising the one or more disbursement amounts; and

the third cryptographic signature;

publishing the inchoate disbursement transaction record;

reading the inchoate disbursement transaction record;

reading the fourth private key from the third key pair sector;

computing a fourth cryptographic signature from the fourth private key;

creating a complete disbursement transaction record comprising:

the commit input;

the one or more disbursement outputs;

the third cryptographic signature; and

the fourth cryptographic signature; and

creating a disbursement transaction by submitting the complete disbursement transaction record to the transfer mechanism.

In the rejection of previously presented **Claim 24**, the Office Action, at page 24, acknowledges that "Rosen does not explicitly disclose wherein the transfer mechanism comprises a decentralized currency." Then, the Office Action alleges that "Feigelson teaches wherein the transfer mechanism comprises a decentralized currency (0050-0051)." The Office Action further alleges that "it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the electronic monetary system of Rosen with the creation and use of digital currency of Feigelson for the purpose of maintaining secrecy of information in order to control its value (0003)." Applicant respectfully disagrees.

As acknowledged by the Office Action, Rosen does not teach or suggest facilitating value transfers via a transfer mechanism, the transfer mechanism comprising a decentralized digital currency as claimed.

In contrast to **Claim 24**, the exchange of economic value as described by Rosen requires " a customer trusted agent securely communicating with a first money module, and a merchant trusted agent securely communicating with a second money module," and "a certifying authority" (Rosen, abstract and claim 1). That is, Rosen requires a certifying authority or any trusted agent for the exchange of economic value. Accordingly, Rosen does not even suggest value transfer via a decentralized digital currency as recited in **Claim 24** that does not require any certifying authority or trusted agent.

Further, the electronic-monetary system in Rosen "is a hybrid of currency, check, card payment systems, and electronic funds transfer systems" (Rosen, paragraph [0002]). Additionally, Rosen allows participants to trade bank-backed promises to stand in lieu of confirmed transfers with the expectation those transfers will be completed successfully later: "The system includes a plurality of issuing banks …" (Rosen, paragraph [0032]); … "The issuing banks later utilize inter-bank clearing and settling processes to maintain the monetary balance in the banking system, as is currently practiced by today's banking industry" (Rosen, paragraph [0029]). That is, the system as described by Rosen requires banks to coordinate with each other, *e.g.*, inter-bank clearing and settling processes. In contrast to Rosen, the value transfer via a decentralized digital currency as recited in **Claim 24** requires neither legacy payment systems (*e.g.* currency, check, card payment systems and electronic funds transfer systems), nor banks or clearing process by the banks.

Further still, Rosen relies on the "tamper-proof computer hardware" (Rosen, paragraph [0033]); transmitting of "electronic representation of currency backed by demand deposit accounts at the issuing bank or credit authorizations ...with digital signatures to provide security from unauthorized modification or counterfeiting," (Rosen, paragraph [0034]); and periodic renewal of "the modules and the individual units of electronic money" to provide security from counterfeiting and tampering (Rosen, paragraph [0034]).

In contrast to Rosen, since the method of **Claim 24** is implemented on a decentralized digital currency instead of certifying authority or issuing banks, the claimed method does not rely on any tamper-proof computer hardware or Rosen's instruments for providing security from counterfeiting and tampering. Accordingly, Rosen fails to teach or suggest facilitating value transfers via a transfer mechanism, the transfer mechanism comprising a decentralized digital currency, as recited in **Claim 24**. Thus, it naturally follows that Rosen fails to teach or suggest "creating a first principal transaction by submitting the first principal transaction record to the transfer mechanism [*i.e.* the decentralized digital

currency]," "creating the commit transaction by submitting the commit transaction record to the transfer mechanism [*i.e.* the decentralized digital currency]," and "creating a disbursement transaction by submitting the complete disbursement transaction record to the transfer mechanism [*i.e.* the decentralized digital currency]," as recited in **Claim 24**.

Furthermore, it is respectfully submitted that one of ordinary skill in the art would not have been motivated to combine Rosen and Feigelson as suggested in the Office Action.

Feigelson is related to physical devices carrying a value and being physically delivered in a transaction and a security feature that is provided by Feigelsonis is the security feature for the physical devices via an element that visually obscures the representation of value, a packaging element of the physical device a holographic foil (Feigelson, paragraphs [0004] and [0005], and claim 1). Although Feigelson describes Bitcoins, Feigelson only concerns about the physical and tangible Bitbills's security (physical devices' security) by providing hologram to the Bitbill for anti-counterfeiting (Feigelson, paragraphs [0075]-[0080]). That is, Feigelson merely provides security concerns for the physical devices that carry values but does not relate to the security provided by submitting a transaction records to a transfer mechanism (a decentralized digital currency) as recited in **Claim 24**. Therefore, one of ordinary skill in the art would not have been motivated to combine Rosen and Feigelson as suggested in the Office Action.

Further still, nowhere of the proposed combination of Rosen and Feigelson is there any teaching or suggestion of below emphasized features in amended **Claim 24** which recites, in part:

> ***transmitting terms from a client via a first network interface, the terms comprising:***
> ***at least one of a first principal amount or a second principal amount;***
> ***a reference to at least one of a first data source or a second data source; and***
> ***an expiration timestamp;***
> receiving the terms at a facilitator via a second network interface;

computing one or more disbursement amounts by applying a disbursement function to:

at least one of the first principal amount or the second principal amount, and

a value from at least one of the first data source or the second data source;

reading the first private key from the first key pair sector;

computing a first cryptographic signature from the first private key;

creating a first principal transaction record comprising:

a first principal output comprising the first principal amount; and

the first cryptographic signature;

creating a first principal transaction by submitting the first principal transaction record to the transfer mechanism;

reading the second private key from the second key pair sector;

computing a second cryptographic signature from the second private key;

creating a commit transaction record comprising:

a first principal input for receiving the first principal amount from the first principal transaction;

a commit output comprising a commit amount; and

the second cryptographic signature;

creating the commit transaction by submitting the commit transaction record to the transfer mechanism;

retrieving a value from the first data source;

reading the third private key from the second key pair sector;

computing a third cryptographic signature from the second private key;

creating an inchoate disbursement transaction record comprising:

a commit input for receiving a commit amount from a commit transaction;

one or more disbursement outputs comprising the one or more disbursement amounts; and

the third cryptographic signature;

publishing the inchoate disbursement transaction record;

reading the inchoate disbursement transaction record;

reading the fourth private key from the third key pair sector;

computing a fourth cryptographic signature from the fourth private key;

creating a complete disbursement transaction record comprising:

the commit input;

the one or more disbursement outputs;

the third cryptographic signature; and

the fourth cryptographic signature; and

creating a disbursement transaction by submitting the complete disbursement transaction record to the transfer mechanism.

Further still, for at least the same reasons that independent **Claim 24** is patentable over the cited reference, it is respectfully submitted that **Claims 1 and 12** is also patentable, to the extent that **Claims 1 and 12** recite similar features as **Claim 24**. Accordingly, for at least the reasons set forth above regarding **Claim 24**, it is respectfully submitted that Rosen and Feigelson, either alone or in combination, fails to teach or suggest all the features of **Claims 1 and 11**; and, therefore, it is respectfully requested that the rejections be reconsidered and withdrawn.

Dependent **Claims 3-6, 9, 15-17, 20, 23, 26, 28, 29 and 31** depend, directly or indirectly, from independent **Claims 1, 11 and 14**, respectively. Accordingly, the dependent claims are allowable over the cited references at least by virtue of their dependency from independent **Claims 1, 11 and 14**, as well as the other features recited therein. It is therefore respectfully requested that rejections under 35 U.S.C. §§ 102(a) and 103 be reconsidered and withdrawn.

CONCLUSION

It is respectfully submitted that the other references in the record do not compensate for the deficiencies of the references utilized in rejecting the pending claims.

It should also be noted that although arguments have been presented with respect to certain claims herein, the recited subject matter as well as various other subject matter and/or combinations of subject matter may be patentable for other reasons. Further, the failure to address any statement by the Examiner herein should not be interpreted as acquiescence or agreement with such statement. Applicant expressly reserves the right to set forth additional and/or alternative reasons for patentability and/or allowance with the present Application or in any other future proceeding, and to rebut any statement presented by the Examiner in this or other papers during prosecution of the present Application.

All objections and rejections having been addressed, it is respectfully submitted that the present application is in condition for allowance, and therefore issuance of a Notice to that effect is earnestly solicited.

Respectfully submitted,

Brundidge & Stanger, PC

Dated: March 11, 2020

/Misung Lee/
Misung Lee
Reg. No. 78,307

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 15/309,612	Filing Date 11/08/2016	☐ 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 $40 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $210 =	
☐ 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	03/11/2020	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 17	Minus	** 30	= 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".	/RENEE M COLLINS/
*** 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.

Electronic Patent Application Fee Transmittal

Application Number:	15309612
Filing Date:	08-Nov-2016
Title of Invention:	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers
First Named Inventor/Applicant Name:	Reginald Middleton
Filer:	Misung Lee/Juel Clyne
Attorney Docket Number:	4675.1002BS

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($)
Miscellaneous:				
RCE- 1ST REQUEST	2801	1	650	650
		Total in USD ($)		**650**

PTO/SB/08a (02-18)
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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	15309612
Filing Date	2016-11-08
First Named Inventor	Reginald Middleton
Art Unit	3685
Examiner Name	NIGH, JAMES D
Attorney Docket Number	4675.1002BS

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15309612
	Filing Date	2016-11-08
	First Named Inventor	Reginald Middleton
	Art Unit	3685
	Examiner Name	NIGH, JAMES D
	Attorney Docket Number	4675.1002BS

	1	Christian Decker, et al "Information Propagation in the Bitcoin Network", 13th IEEE International Conference on Peer-to-Peer Computing", 978-1-4799-0521, August 2013, pages 1-10.

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15309612
	Filing Date	2016-11-08
	First Named Inventor	Reginald Middleton
	Art Unit	3685
	Examiner Name	NIGH, JAMES D
	Attorney Docket Number	4675.1002BS

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Misung Lee/	Date (YYYY-MM-DD)	2020-03-13
Name/Print	Misung Lee	Registration Number	78307

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1 hour 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.**

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 record s.

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 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.

Electronic Acknowledgement Receipt

EFS ID:	38857595
Application Number:	15309612
International Application Number:	
Confirmation Number:	2321
Title of Invention:	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers
First Named Inventor/Applicant Name:	Reginald Middleton
Customer Number:	86636
Filer:	Misung Lee/Juel Clyne
Filer Authorized By:	Misung Lee
Attorney Docket Number:	4675.1002BS
Receipt Date:	13-MAR-2020
Filing Date:	08-NOV-2016
Time Stamp:	12:04:56
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	Information Disclosure Statement (IDS) Form (SB08)	4675_IDS.pdf	1034505 a7040966bbede54e035d0163c464cb987c607d58	no	4

Warnings:

Information:					
A U.S. Patent Number Citation or a U.S. Publication Number Citation is required in the Information Disclosure Statement (IDS) form for autoloading of data into USPTO systems. You may remove the form to add the required data in order to correct the Informational Message if you are citing U.S. References. If you chose not to include U.S. References, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.					
2	Non Patent Literature	P2P2013_041.pdf	330720 deb1c04f3584a59b489e9582b244c10c7f9b20cf	no	10
Warnings:					
Information:					
			Total Files Size (in bytes):	1365225	

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.

Notice of References Cited	Application/Control No. 15/309,612	Applicant(s)/Patent Under Reexamination Middleton et al.	
	Examiner JAMES D NIGH	Art Unit 3685	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-20130166455-A1	06-2013	Feigelson; Douglas	G06Q30/06	705/64
*	B	US-20030070080-A1	04-2003	Rosen, Sholom S.	G06Q20/06	713/187
	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	
	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.

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (02-18)
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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	15309612
Filing Date	2016-11-08
First Named Inventor	Reginald Middleton
Art Unit	3685
Examiner Name	NIGH, JAMES D
Attorney Docket Number	4675.1002BS

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.D.N/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15309612
	Filing Date	2016-11-08
	First Named Inventor	Reginald Middleton
	Art Unit	3685
	Examiner Name	NIGH, JAMES D
	Attorney Docket Number	4675.1002BS

	1	Christian Decker, et al "Information Propagation in the Bitcoin Network", 13th IEEE International Conference on Peer-to-Peer Computing", 978-1-4799-0521, August 2013, pages 1-10.

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/JAMES D NIGH/	Date Considered	06/05/2020

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.D.N/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	15309612
Filing Date	2016-11-08
First Named Inventor	Reginald Middleton
Art Unit	3685
Examiner Name	NIGH, JAMES D
Attorney Docket Number	4675.1002BS

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Misung Lee/	Date (YYYY-MM-DD)	2020-03-13
Name/Print	Misung Lee	Registration Number	78307

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1 hour 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.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.D.N/

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 record s.

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 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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.D.N/

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.
15/309,612	11/08/2016	Reginald Middleton	4675.1002BS	2321

86636 7590 06/08/2020

BRUNDIDGE & STANGER, P.C.
1925 BALLENGER AVENUE, STE. 560
ALEXANDRIA, VA 22314

EXAMINER	
NIGH, JAMES D	

ART UNIT	PAPER NUMBER
3685	

MAIL DATE	DELIVERY MODE
06/08/2020	PAPER

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.

Office Action Summary	Application No. 15/309,612	Applicant(s) Middleton et al.	
	Examiner JAMES D NIGH	Art Unit 3685	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 13 March 2020.

☐ 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) 1,3-6,9,12,15-17,20,23-24,26,28-29 and 31 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) 1,3-6,9,12,15-17,20,23-24,26,28-29 and 31 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 03/13/2020.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

DETAILED ACTION

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.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on March 11, 2020 has been entered.

Claim Status

3. As of the Office Action dated December 11, 2019 claims 1 through 30 were pending and claims 1 through 30 stood rejected. Claims 1, 3-5, 9, 12, 15-17, 20, 23-24, 26 and 28 have been amended. Claims 2, 7, 8, 10, 11, 13, 14, 18, 19, 21, 22, 25, 27 and 30 have been cancelled. Claim 31 has been added. Claims 1, 3-6, 9, 12, 15-17, 20, 23-24, 26, 28, 29 and 31 are therefore currently pending and are presented for examination on the merits.

Information Disclosure Statement

4. The information disclosure statement (IDS) was submitted on March 13, 2020. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Response to Arguments

5. Applicant's argument with regard to the 35 U.S.C. § 112 (a) or 35 U.S.C. § 112 (pre-AIA) 1st paragraph rejection of claims 13, 27 and 30 has been fully considered and is persuasive. Accordingly the rejection is being withdrawn.

6. Applicant's argument with regard to the 35 U.S.C. § 112 (b) or 35 U.S.C. § 112 (pre-AIA) 2nd paragraph rejection of claims 13, 27 and 30 has been fully considered and is persuasive. Accordingly the rejection is being withdrawn.

7. Applicant's argument with regard to the 35 U.S.C. § 112 (d) or 35 U.S.C. § 112 (pre-AIA) 4th paragraph rejection of claims 13, 27 and 30 has been fully considered and is persuasive. Accordingly the rejection is being withdrawn.

8. Applicant's argument with regard to the 35 U.S.C. § 103 (a) rejection of claim 24 has been fully considered but is not persuasive. The claim is not claiming the actual mechanisms for implementing a decentralized currency such as the distributed ledger or blockchain but only the intermediary serving to bring agreement and administer the contract between a first party and a second party that involves exchange of value inclusive of a decentralized currency. As such the facilitator clearly is playing a centralized role even if the currency is a decentralized currency and nothing within the claim itself or even the written disclosure of the examined application suggests that the role of the facilitator would in any way be altered based on whether the currency was centralized or decentralized. Paragraph 29 of the filed application teaches that combinations between centralized and decentralized currencies are possible and nothing within the claim itself or the written disclosure would suggest that the limiting of the operations to only involve decentralized currency would constitute anything more than a field of use which would not distinguish the claim from the prior art. Furthermore

given the breadth of the teachings of the Rosen disclosure nothing is present that would suggest that the functions of administrating contracts and payments would be altered based on the nature of the underlying currency. As such those skilled in the art would view Rosen when combined with Feigelson as simply adding a feature not present in Rosen that would entail nothing more than bringing about a predictable result. No specialized teaching is required to add the capability of cryptocurrency to Rosen. As noted in MPEP § 2144 (II) "...the desire to enhance commercial opportunities by improving a product or process is universal—and even common-sensical" and those skilled in the art upon seeing an additional commercial opportunity to enhance Rosen would certainly have relied on Rosen or a similar reference in order to provide the additional capability of interfacing with a cryptocurrency. Applicant merely makes piecemeal arguments against individual references when a combination of references was cited. As such the present rejection will be maintained. With regard to claims 1 and 12 as the argument relies on the alleged deficiencies of Rosen in view of Feigelson as applied to claim 24 the argument is equally unpersuasive as is the argument with regard to dependent claims 3-6, 9, 15-17, 20, 23, 26, 28, 29 and 31.

Claim Rejections - 35 USC § 101

9. 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.

10. Claims 1, 3-6, 9, 12, 15-17, 20, 23-24, 26, 28, 29 and 31 are rejected under 35 U.S.C. 101 because the claimed invention is directed to an abstract idea without significantly more.

11. Claim 1 recites a device and therefore meets Step 1 of the 2019 Revised Patent Subject Matter Eligibility Guidance as it can be viewed as a machine which falls within one of the four categories of statutory subject matter. Claim 1 recites as follows:

1. (Currently Amended) A device for facilitating a value transfer between a first party utilizing a first client and a second party utilizing a second client via a transfer mechanism, the transfer mechanism comprising a decentralized digital currency, the device comprising:

a first memory comprising a transaction record sector and a first key pair sector for storing a first asymmetric key pair, the first asymmetric key pair comprising a first private key and a first public key;

a first network interface for receiving terms, the terms comprising:

at least one of a first principal amount or a second principal amount;

a reference to at least one of a first data source or a second data source; and

an expiration timestamp;

a first computer processor coupled to the first memory and the first network interface, the first computer processor configured to:

compute one or more disbursement amounts by applying a disbursement function to:

at least one of the first principal amount or the second principal amount, and

a value from at least one of the first data source or the second data source;

read the first private key from the first key pair sector;

compute a first cryptographic signature from the first private key;

create an inchoate disbursement transaction record comprising:

a commit input for receiving a commit amount from a commit transaction;

one or more disbursement outputs comprising the disbursement amounts; and

the first cryptographic signature; and

publish the inchoate disbursement transaction record to at least one of the first client and the second client;

where the first client comprises:

a second memory comprising a second key pair sector for storing a second asymmetric key pair, the second asymmetric key pair comprising a second private key and a second public key;

a second network interface; and

a second computer processor coupled to the second memory and the second network interface, the second computer processor configured to;

read the second private key from the second key pair sector;

read the inchoate disbursement transaction record; compute a second cryptographic signature from the second private key;

create a complete disbursement transaction record comprising:

the commit input;

the disbursement outputs;

the first cryptographic signature; and

the second cryptographic signature; and

create a disbursement transaction by submitting the complete disbursement transaction record to the transfer mechanism; and

where the second client comprises;

a third memory comprising a third key pair sector for storing a third asymmetric key pair, the third asymmetric key pair comprising a third private key and a third public key;

a third network interface; and

a third computer processor coupled to the third memory and the third network interface, the third computer processor configured to read the third private key from the third key pair sector.

The claim is analyzed under prong one, step 2A in order to determine if the claim is directed towards a judicial exception. The claim recites in the preamble that it is directed towards a value transfer between a first party and a second party. Transaction records and asymmetric key pairs are used and terms are received comprising a first or second principal amount, a reference to one of two data sources and an expiration time stamp. Disbursement amounts are computed by applying a disbursement function to at least one of the two principal amounts and a value from at least one of two data sources. A private key is retrieved and is used to compute a cryptographic signature. A transaction record is then formed by receiving a commit amount, one or more disbursement amounts and the computed cryptographic signature and the record is then published to at least one of a first and second client. Although the claim per the preamble is only directed towards a device for facilitating a value transfer between a first party utilizing a first client and a second party utilizing a second client, the claim further goes on to describe structure and operations associated with the first and second client. The first client reads a second private key and the transaction record and computes a second cryptographic signature from the second private key and creates a

complete disbursement record comprising the commit input, the disbursement outputs and the first and second cryptographic signatures and creates a disbursement transaction by submitting the disbursement record to the transfer mechanism. The second client is recited as storing public and private keys and reading the private key. The claim falls within two groupings of abstract ideas involving the organizing of human activity as indicated in the 2019 Revised Patent Subject Matter Eligibility Guidance, one of which is the processing of a payment between two parties which falls under the category of a fundamental economic practice. As the claim also recites that the transaction requires particular signatures of the intermediary and the first client the claim can also be viewed as falling within the category of a commercial/legal interaction involving a contract involving terms including principal amounts, references to data sources and expiration of the terms i.e. requiring that the contract be consummated within a specified period of time that result in the creation of a disbursement transaction record including amounts, values, signatures and commitment inputs that are then published to both parties to the contract. The disclosure itself recites at paragraph 108 that "The invention pertains to agreements among distinct parties that contemplate transfer of title to property, as well as any industry where that may be of value or importance" and clearly falls within the grouping of commercial/legal interactions under the groupings. Therefore under the analysis made under prong one of step 2A the claim is determined to be ineligible.

The analysis then proceeds to prong two of step 2A where an analysis is performed in order to determine whether the claim recites additional elements that integrate the abstract idea into a practical application of the abstract idea. Integrating

the claim into a practical application requires an additional element or a combination of additional elements in the claim to apply, rely on, or use the judicial exception in a manner that imposes a meaningful limit on the judicial exception, such that the claim is more than a drafting effort designed to monopolize the exception. The structural elements in the claim include the memory of the claimed device, a network interface and a processor. The claim also recites that the device possesses the capability of encryption by taking a private key and computing a cryptographic signature. In reviewing the written disclosure at paragraphs 52-53, 106 and 113 the processor, memory and network interface are described in a manner that includes no technological improvement to the functioning of the processor and only describes a particular technological environment for which an intermediary described in paragraph 113 as a "facilitator" is linked. With regard to the encryption capabilities no particular algorithm for computing a signature is described in the written disclosure beyond the recitations at pages 17, 18 and 28 that in order to consummate a transaction that a plurality of signatures are required and the function is described at a generally high level by the written disclosure such that in the broadest reasonable interpretation the claim scope encompasses encryption that could be performed by human beings. Even if a computer calculation of the signature were inferred from the claim the written disclosure relies on prior art signature calculation mechanisms such as multisignature transactions (see footnote 2 of page 4 of the written disclosure) or P2SH (97 and 104 of the written disclosure) and therefore do not constitute any technological improvement to the functioning of the computer itself. While the claim scope is limited in scope to the device acting as a facilitator or intermediary Examiner will also consider the two clients

participation. The first client also comprises a memory, a network interface and a processor and is also performing a computation of a cryptographic signature using a private key. The second client also comprises a memory, a network interface and a processor. As pointed out paragraphs 52-53 and 106 of the written disclosure are directed towards a generic computing environment that include no technological improvement to the functioning of any particular computer and paragraph 110 in describing the client also describes a generic computing device with no technological improvement. If the combination of facilitator and two clients are considered there is no meaningful technological contribution being made as the facilitator and clients merely represent the computer equivalents of two parties to a contract in which an intermediary is used and therefore the combination as a whole is merely a mechanism for linking the abstract idea to a particular technological environment. Therefore under prong two of Step 2A no practical application of the abstract idea is present in the claim and the result of the analysis is that the claim is still ineligible.

Dependent claims 3-6 and 9 recite the same elements as claim 1 inclusive of different data but utilize the same structural components and signature computation present in claim 1. Therefore under both prongs one and two of Step 2A these limitations only serve to add additional layers of abstraction to the abstract idea of claim 1 and therefore under prongs one and two of step 2A are also found to be ineligible.

The analysis proceeds to step 2B of the 2019 Revised Patent Subject Matter Eligibility Guidance. The claim recites structural elements in the claim including the memory of the claimed device, a network interface and a processor. The claim also recites that the device possesses the capability of encryption by taking a private key

and computing a cryptographic signature. In reviewing the written disclosure at paragraphs 52-53, 106 and 113 the processor, memory and network interface are described in a manner that includes no technological improvement to the functioning of the processor and only describes a particular technological environment for which an intermediary described in paragraph 113 as a "facilitator" is linked. With regard to the encryption capabilities no particular algorithm for computing a signature is described in the written disclosure beyond the recitations at pages 17, 18 and 28 that in order to consummate a transaction that a plurality of signatures are required and the function is described at a generally high level by the written disclosure such that in the broadest reasonable interpretation the claim scope encompasses encryption that could be performed by human beings. Even if a computer calculation of the signature were inferred from the claim the written disclosure relies on prior art signature calculation mechanisms such as multisignature transactions (see footnote 2 of page 4 of the written disclosure) or P2SH (97 and 104 of the written disclosure) and therefore do not constitute any technological improvement to the functioning of the computer itself. While the claim scope is limited in scope to the device acting as a facilitator or intermediary Examiner will also consider the two client's participation. The first client also comprises a memory, a network interface and a processor and is also performing a computation of a cryptographic signature using a private key. The second client also comprises a memory, a network interface and a processor. As pointed out paragraphs 52-53 and 106 of the written disclosure are directed towards a generic computing environment that include no technological improvement to the functioning of any particular computer and paragraph 110 in describing the client also describes a generic

computing device with no technological improvement. If the combination of facilitator and two clients are considered there is no meaningful technological contribution being made as the facilitator and clients merely represent the computer equivalents of two parties to a contract in which an intermediary is used and therefore the combination as a whole is merely a mechanism for linking the abstract idea to a particular technological environment. No technological improvement is recited to the recited device, nor does the combination of device and two clients serve to form an ordered combination of elements that results in any technological improvement. It is abundantly clear that the claim does not involve any ordered combination of elements as the recited device does not utilize any special properties of a network or distributed computing in order to gain any technological improvement and merely are directed towards a centralized, "one-size-fits-all" technological implementation and the clients merely serve as representatives of human counterparts engaging in a contract (*BASCOM Glob. Internet Servs. v. AT&T Mobility, LLC*, 119 USPQ2d 1236 (Fed. Cir. 2016)). It is also clear that no similarity is present with regard to *McRO* (*McRO, Inc. v. Bandai Namco Games Am. Inc.*, 120 USPQ2d 1091 (Fed. Cir. 2016)) as the process applied in McRO which involved the evaluation of a plurality of subsequences of phonemes in order to set morph weights and was a process that was not previously used by human beings in performing lip synchronization between the animated characters and the reproduced sounds. While *McRO* acknowledged that human beings could perform the operations recited in the steps it was also clear that human beings had never previously acted in such a manner, particularly as it applied to the evaluation of subsequences of phonemes in order to set the morph weights. However in the instant claims the recited

operations of transferring payments and utilizing trusted intermediaries in making a payment are all operations that have previously been done by human beings in the same manner being claimed. It is also clear that there is no similarity to *DDR Holdings* (*DDR Holdings, LLC v. Hotels.com, LP*, 113 USPQ2d 1097 (Fed. Cir. 2014)) as there is nothing in the claims themselves or even in the written description to explicitly state or even implicitly suggest that the claims involve anything more than generic computer operations. It is also clear that there is no similarity to *Enfish* (*Enfish, LLC v. Microsoft Corp.*, 118 USPQ2d 1684 (Fed. Cir. 2016)) because nothing within the claim or the four corners of the written description provides any teaching or suggestion of an improved computer algorithm for analyzing data such as the self-referential table of *Enfish* that brings about an improvement to the computer itself where *Enfish* taught that the claimed invention brought about "increased flexibility, faster search times, and smaller memory requirements" (*Enfish* at 1690). There is also no technological improvement being made to any external technology (*Diamond v. Diehr*, 450 U.S. 175, 184 (1981)). The written disclosure at paragraphs 52-53, 106, 110 and 113 describe only the use of a generic unimproved computing environment and describes the elements in a manner that indicates that the additional elements are sufficiently well-known that the specification does not need to describe the particulars of such additional elements to satisfy 35 U.S.C. §112 (a) ("In other words, the claims in *Diehr* were patent eligible because they improved an existing technological process, not because they were implemented on a computer", *Alice* at 1983). Therefore it is clear that no inventive concept is present sufficient to confer eligibility in light of the fact that the claims are

clearly directed towards an abstract idea. Therefore claims 1, 3-6 and 9 are rejected under 35 U.S.C. § 101 as being directed towards ineligible subject matter.

12. Claim 12 recites a system and therefore meets Step 1 of the 2019 Revised Patent Subject Matter Eligibility Guidance as it can be viewed as a product which falls within one of the four categories of statutory subject matter. Claim 12 recites as follows:

12. (Currently Amended) A system for facilitating a value transfer between a first party utilizing a first client and a second party utilizing a second client via a transfer mechanism, the transfer mechanism comprising a decentralized digital currency, the system comprising a facilitator, the first client, and the second client; the facilitator comprising:

a first memory comprising a transaction record sector and a first key pair sector for storing a first asymmetric key pair, the first asymmetric key pair comprising a first private key and a first public key;

a first network interface for receiving terms, the terms comprising:

at least one of a first principal amount or a second principal amount;

a reference to at least one of a first data source or a second data source; and

an expiration timestamp; and

a first computer processor coupled to the first memory and the first network interface, the first computer processor configured to:

compute one or more disbursement amounts by applying a disbursement function to:

at least one of the first principal amount or the second principal amount, and

a value from at least one of the first data source or the second data source;

read the first private key from the first key pair sector;

compute a first cryptographic signature from the first private key;

create an inchoate disbursement transaction record comprising:

a commit input for receiving a commit amount from a commit transaction;

one or more disbursement outputs comprising the disbursement amounts; and

the first cryptographic signature; and

publish the inchoate disbursement transaction record to at least one of the first client and the second client;

the first client comprising:

a second memory comprising a second key pair sector for storing a second asymmetric key pair, the second asymmetric key pair comprising a second private key and a second public key;

a second network interface; and

a second computer processor coupled to the second memory and the second network interface, the second computer processor configured to; read the second private key from the second key pair sector;

read the inchoate disbursement transaction record;

compute a second cryptographic signature from the second private key;

create a complete disbursement transaction record comprising:

the commit input;

the disbursement outputs;

the first cryptographic signature; and

the second cryptographic signature; and

create a disbursement transaction by submitting the complete disbursement transaction record to the transfer mechanism; and

the second client comprising:

a third memory comprising a third key pair sector for storing a third asymmetric key pair, the third asymmetric key pair comprising a third private key and a third public key;

a third network interface; and

a third computer processor coupled to the third memory and the third network interface, the third computer processor configured to read the third private key from the third key pair sector.

The claim is analyzed under prong one, step 2A in order to determine if the claim is directed towards a judicial exception. The claim recites in the preamble that it is directed towards a value transfer between a first party and a second party. Transaction records and asymmetric key pairs are used and terms are received comprising a first or second principal amount, a reference to one of two data sources and an expiration time stamp. Disbursement amounts are computed by applying a disbursement function to at least one of the two principal amounts and a value from at least one of two data sources. A private key is retrieved and is used to compute a cryptographic signature. A transaction record is then formed by receiving a commit amount, one or more disbursement amounts and the computed cryptographic signature and the record is then published to at least one of a first and second client. The system includes a device for facilitating a value transfer between a first party utilizing a first client and a second party utilizing a second client. The first client reads a second private key and the

transaction record and computes a second cryptographic signature from the second private key and creates a complete disbursement record comprising the commit input, the disbursement outputs and the first and second cryptographic signatures and creates a disbursement transaction by submitting the disbursement record to the transfer mechanism. The second client is recited as storing public and private keys and reading the private key. The claim falls within two groupings of abstract ideas involving the organizing of human activity as indicated in the 2019 Revised Patent Subject Matter Eligibility Guidance, one of which is the processing of a payment between two parties which falls under the category of a fundamental economic practice. As the claim also recites that the transaction requires particular signatures of the intermediary and the first client the claim can also be viewed as falling within the category of a commercial/legal interaction involving a contract involving terms including principal amounts, references to data sources and expiration of the terms i.e. requiring that the contract be consummated within a specified period of time that result in the creation of a disbursement transaction record including amounts, values, signatures and commitment inputs that are then published to both parties to the contract. The disclosure itself recites at paragraph 108 that “The invention pertains to agreements among distinct parties that contemplate transfer of title to property, as well as any industry where that may be of value or importance” and clearly falls within the grouping of commercial/legal interactions under the groupings. Therefore under the analysis made under prong one of step 2A the claim is determined to be ineligible.

The analysis then proceeds to prong two of step 2A where an analysis is performed in order to determine whether the claim recites additional elements that

integrate the abstract idea into a practical application of the abstract idea. Integrating the claim into a practical application requires an additional element or a combination of additional elements in the claim to apply, rely on, or use the judicial exception in a manner that imposes a meaningful limit on the judicial exception, such that the claim is more than a drafting effort designed to monopolize the exception. The structural elements in the claim include the memory of the claimed facilitator further including a network interface and a processor, the first client including a memory, a network interface and a processor and a second client including a memory, a network interface and a processor. The claim also recites that the facilitator device and the first client possess the capability of encryption by taking a private key and computing a cryptographic signature. In reviewing the written disclosure at paragraphs 52-53, 106 and 113 the processor, memory and network interface of the facilitator device are described in a manner that includes no technological improvement to the functioning of the processor and only describes a particular technological environment for which an intermediary described in paragraph 113 as a "facilitator" is linked. With regard to the encryption capabilities no particular algorithm for computing a signature is described in the written disclosure beyond the recitations at pages 17, 18 and 28 that in order to consummate a transaction that a plurality of signatures are required and the function is described at a generally high level by the written disclosure such that in the broadest reasonable interpretation the claim scope encompasses encryption that could be performed by human beings. Even if a computer calculation of the signature were inferred from the claim the written disclosure relies on prior art signature calculation mechanisms such as multisignature transactions (see footnote 2 of page 4 of the written

disclosure) or P2SH (97 and 104 of the written disclosure) and therefore do not constitute any technological improvement to the functioning of the computer itself. With regard to the two clients the first client also comprises a memory, a network interface and a processor and is also performing a computation of a cryptographic signature using a private key. The second client also comprises a memory, a network interface and a processor. As pointed out paragraphs 52-53 and 106 of the written disclosure are directed towards a generic computing environment that include no technological improvement to the functioning of any particular computer and paragraph 110 in describing the client also describes a generic computing device with no technological improvement. If the combination of facilitator and two clients are considered there is no meaningful technological contribution being made in the form of a combination of elements as the facilitator and clients merely represent the computer equivalents of two parties to a contract in which an intermediary is used and therefore the combination as a whole is merely a mechanism for linking the abstract idea to a particular technological environment. Therefore under prong two of Step 2A no practical application of the abstract idea is present in the claim and the result of the analysis is that the claim is still ineligible.

Dependent claims 15-17, 20 and 23 recite the same elements as claim 12 inclusive of different data but utilize the same structural components and signature computation present in claim 12. Therefore under both prongs one and two of Step 2A these limitations only serve to add additional layers of abstraction to the abstract idea of claim 1 and therefore under prongs one and two of step 2A are also found to be ineligible.

The analysis proceeds to step 2B of the 2019 Revised Patent Subject Matter Eligibility Guidance. The claim recites structural elements in the claim including the memory of the claimed facilitator device further including a network interface and a processor and two client devices also including a memory, a network interface and a processor. The claim also recites that the facilitator device and the first client possess the capability of encryption by taking a private key and computing a cryptographic signature. In reviewing the written disclosure at paragraphs 52-53, 106 and 113 the processor, memory and network interface are described in a manner that includes no technological improvement to the functioning of the processor and only describes a particular technological environment for which an intermediary described in paragraph 113 as a "facilitator" is linked. With regard to the encryption capabilities no particular algorithm for computing a signature is described in the written disclosure beyond the recitations at pages 17, 18 and 28 that in order to consummate a transaction that a plurality of signatures are required and the function is described at a generally high level by the written disclosure such that in the broadest reasonable interpretation the claim scope encompasses encryption that could be performed by human beings. Even if a computer calculation of the signature were inferred from the claim the written disclosure relies on prior art signature calculation mechanisms such as multisignature transactions (see footnote 2 of page 4 of the written disclosure) or P2SH (97 and 104 of the written disclosure) and therefore do not constitute any technological improvement to the functioning of the computer itself. The first client also comprises a memory, a network interface and a processor and is also performing a computation of a cryptographic signature using a private key. The second client also comprises a memory, a network

interface and a processor. As pointed out paragraphs 52-53 and 106 of the written disclosure are directed towards a generic computing environment that include no technological improvement to the functioning of any particular computer and paragraph 110 in describing the client also describes a generic computing device with no technological improvement. If the combination of facilitator and two clients are considered there is no meaningful technological contribution being made as the facilitator and clients merely represent the computer equivalents of two parties to a contract in which an intermediary is used and therefore the combination as a whole is merely a mechanism for linking the abstract idea to a particular technological environment. No technological improvement is recited to the recited facilitator device or the two client devices nor does the combination of device and two clients serve to form an ordered combination of elements that results in any technological improvement. It is abundantly clear that the claim does not involve any ordered combination of elements as the recited facilitator device along with the two clients do not utilize any special properties of a network or distributed computing in order to gain any technological improvement and merely are directed towards a centralized, "one-size-fits-all" technological implementation and the clients merely serve as representatives of human counterparts engaging in a contract (*BASCOM Glob. Internet Servs. v. AT&T Mobility, LLC*, 119 USPQ2d 1236 (Fed. Cir. 2016)). It is also clear that no similarity is present with regard to *McRO* (*McRO, Inc. v. Bandai Namco Games Am. Inc.*, 120 USPQ2d 1091 (Fed. Cir. 2016)) as the process applied in McRO which involved the evaluation of a plurality of subsequences of phonemes in order to set morph weights and was a process that was not previously used by human beings in performing lip synchronization

between the animated characters and the reproduced sounds. While *McRO* acknowledged that human beings could perform the operations recited in the steps it was also clear that human beings had never previously acted in such a manner, particularly as it applied to the evaluation of subsequences of phonemes in order to set the morph weights. However in the instant claims the recited operations of transferring payments and utilizing trusted intermediaries in making a payment are all operations that have previously been done by human beings in the same manner being claimed. It is also clear that there is no similarity to *DDR Holdings* (*DDR Holdings, LLC v. Hotels.com, LP*, 113 USPQ2d 1097 (Fed. Cir. 2014)) as there is nothing in the claims themselves or even in the written description to explicitly state or even implicitly suggest that the claims involve anything more than generic computer operations. It is also clear that there is no similarity to *Enfish* (*Enfish, LLC v. Microsoft Corp.*, 118 USPQ2d 1684 (Fed. Cir. 2016)) because nothing within the claim or the four corners of the written description provides any teaching or suggestion of an improved computer algorithm for analyzing data such as the self-referential table of *Enfish* that brings about an improvement to the computer itself where *Enfish* taught that the claimed invention brought about "increased flexibility, faster search times, and smaller memory requirements" (*Enfish* at 1690). There is also no technological improvement being made to any external technology (*Diamond v. Diehr*, 450 U.S. 175, 184 (1981)). The written disclosure at paragraphs 52-53, 106, 110 and 113 describe only the use of a generic unimproved computing environment and describes the elements in a manner that indicates that the additional elements are sufficiently well-known that the specification does not need to describe the particulars of such additional elements to

satisfy 35 U.S.C. §112 (a) ("In other words, the claims in *Diehr* were patent eligible because they improved an existing technological process, not because they were implemented on a computer", *Alice* at 1983). Therefore it is clear that no inventive concept is present sufficient to confer eligibility in light of the fact that the claims are clearly directed towards an abstract idea. Therefore claims 12, 15-17, 20 and 23 are rejected under 35 U.S.C. § 101 as being directed towards ineligible subject matter.

13. Claim 24 recites a method and therefore meets Step 1 of the 2019 Revised Patent Subject Matter Eligibility Guidance as it can be viewed as a product which falls within one of the four categories of statutory subject matter. Claim 24 recites as follows:

24. (Currently Amended) A method for facilitating value transfers between a first party utilizing a first client and a second party utilizing a second client via a transfer mechanism, the transfer mechanism comprising a decentralized digital currency, the method comprising:

storing a first asymmetric key pair in a first key pair sector of a first memory, the first asymmetric key pair comprising a first private key and a first public key;

storing a second asymmetric key pair in a second key pair sector of a second memory, the second asymmetric key pair comprising a second private key and a second public key;

storing a third asymmetric key pair in the second key pair sector, the third key pair comprising a third private key and a third public key;

storing a fourth asymmetric key pair in a third key pair sector of a third memory, the fourth asymmetric key pair comprising a fourth private key and a fourth public key;

transmitting terms from one of the first or second client via a first network interface, the terms comprising:

at least one of a first principal amount or a second principal amount;

a reference to at least one of a first data source or a second data source; and

an expiration timestamp;

receiving the terms at a facilitator via a second network interface;

computing one or more disbursement amounts by applying a disbursement function to: at least one of the first principal amount or the second principal amount, and

a value from at least one of the first data source or the second data source;

reading the first private key from the first key pair sector;

computing a first cryptographic signature from the first private key;

creating a first principal transaction record comprising:

a first principal output comprising the first principal amount; and

the first cryptographic signature;

creating a first principal transaction by submitting the first principal transaction record to the transfer mechanism;

reading the second private key from the second key pair sector;

computing a second cryptographic signature from the second private key;

creating a commit transaction record comprising:

a first principal input for receiving the first principal amount from the first principal transaction;

a commit output comprising a commit amount; and

the second cryptographic signature;

creating the commit transaction by submitting the commit transaction record to the transfer mechanism;

retrieving a value from the first data source;

reading the third private key from the second key pair sector;

computing a third cryptographic signature from the second private key;

creating an inchoate disbursement transaction record comprising:

a commit input for receiving a commit amount from a commit transaction;

one or more disbursement outputs comprising the one or more disbursement amounts; and

the third cryptographic signature;

publishing the inchoate disbursement transaction record;

reading the inchoate disbursement transaction record;

reading the fourth private key from the third key pair sector;

computing a fourth cryptographic signature from the fourth private key;

creating a complete disbursement transaction record comprising:

the commit input;

the one or more disbursement outputs;

the third cryptographic signature; and

the fourth cryptographic signature; and

creating a disbursement transaction by submitting the complete disbursement transaction record to the transfer mechanism.

The claim is analyzed under prong one, step 2A in order to determine if the claim is directed towards a judicial exception. The claim recites in the preamble that it is

directed towards a value transfer between a first party and a second party. Four asymmetric key pairs are first stored. The first or second client sends terms to a facilitator including a principal amount, reference to a data source and an expiration timestamp. The facilitator receives the terms and computes disbursement amounts including the principal amount and a value from a data store and then reads a private key and computes a cryptographic signature and then creates a first principal transaction record comprising the first principal amount and the cryptographic signature. The first principal transaction record is then submitted to the transfer mechanism. A second private key is read and a second cryptographic signature is computed from the second private key. A commit transaction is then created comprising a first principal input for receiving the first principal amount, a commit output comprising a commit amount and the second cryptographic signature. A value is retrieved, a third private key is read and a third cryptographic signature is computed using a second private key. An inchoate disbursement transaction record is then created comprising a commit input, one or more disbursement outputs comprising disbursement amounts and the third cryptographic signature. The inchoate disbursement transaction record is then published. The inchoate disbursement transaction record is then read. A fourth private key is read, a fourth cryptographic signature is computed and a complete disbursement transaction record is created comprising the commit input, one or more disbursement outputs and the third and fourth cryptographic signature. A disbursement transaction is then created by submitting the complete disbursement transaction record to the transfer mechanism. The claim falls within two groupings of abstract ideas involving the organizing of human activity as indicated in the 2019 Revised Patent Subject Matter

Eligibility Guidance, one of which is the processing of a payment between two parties which falls under the category of a fundamental economic practice. As the claim also recites that the transaction requires particular signatures of the intermediary and the first client the claim can also be viewed as falling within the category of a commercial/legal interaction involving a contract involving terms including principal amounts, references to data sources and expiration of the terms i.e. requiring that the contract be consummated within a specified period of time that result in the creation of a disbursement transaction record including amounts, values, signatures and commitment inputs that are then published to both parties to the contract. The disclosure itself recites at paragraph 108 that "The invention pertains to agreements among distinct parties that contemplate transfer of title to property, as well as any industry where that may be of value or importance" and clearly falls within the grouping of commercial/legal interactions under the groupings. Therefore under the analysis made under prong one of step 2A the claim is determined to be ineligible.

The analysis then proceeds to prong two of step 2A where an analysis is performed in order to determine whether the claim recites additional elements that integrate the abstract idea into a practical application of the abstract idea. Integrating the claim into a practical application requires an additional element or a combination of additional elements in the claim to apply, rely on, or use the judicial exception in a manner that imposes a meaningful limit on the judicial exception, such that the claim is more than a drafting effort designed to monopolize the exception. The structural elements in the claim are limited to what is described as a "transfer mechanism", three memories and two network interfaces along with recitations of first and second clients in

the preamble. The claim also recites the capability of encryption by taking a private key and computing a cryptographic signature. In reviewing the written disclosure at paragraphs 52-53, 106 and 113 the memory and network interface are described in a manner that includes no technological improvement to the functioning of the memory and network interface and only describes a particular technological environment for which an intermediary described in paragraph 113 as a "facilitator" is linked. With regard to the encryption capabilities no particular algorithm for computing a signature is described in the written disclosure beyond the recitations at pages 17, 18 and 28 that in order to consummate a transaction that a plurality of signatures are required and the function is described at a generally high level by the written disclosure such that in the broadest reasonable interpretation the claim scope encompasses encryption that could be performed by human beings. Even if a computer calculation of the signature were inferred from the claim the written disclosure relies on prior art signature calculation mechanisms such as multisignature transactions (see footnote 2 of page 4 of the written disclosure) or P2SH (97 and 104 of the written disclosure) and therefore do not constitute any technological improvement to the functioning of the computer itself. With regard to the two clients paragraph 110 in describing the client also describes a generic computing device with no technological improvement. The transfer mechanism per paragraphs 53, 54 and 96 are not elements of physical structure but instead are protocols involving at least decentralized currency ("Where a decentralized digital currency [e.g., the Bitcoin protocol, the Ethereum protocol, or similar] *is used as the transfer mechanism*...", 96) but per paragraph 49 can also involve centralized currency and the broadest reasonable interpretation of the term transfer mechanism can be

viewed as any form of monetary exchange scheme. If the combination of transfer mechanism, memory, network interfaces and two clients are considered there is no meaningful technological contribution being made in the form of a combination of elements as the transfer mechanism and clients merely represent the computer equivalents of two parties to a contract in which an intermediary is used through the network interfaces and therefore the combination as a whole is merely a mechanism for linking the abstract idea to a particular technological environment. Therefore under prong two of Step 2A no practical application of the abstract idea is present in the claim and the result of the analysis is that the claim is still ineligible.

Dependent claims 26, 28, 29 and 31 recite the same elements as claim 24 inclusive of different data but utilize the same structural components and signature computation present in claim 24. Therefore under both prongs one and two of Step 2A these limitations only serve to add additional layers of abstraction to the abstract idea of claim 1 and therefore under prongs one and two of step 2A are also found to be ineligible.

The analysis proceeds to step 2B of the 2019 Revised Patent Subject Matter Eligibility Guidance. The structural elements in the claim are limited to what is described as a “transfer mechanism”, three memories and two network interfaces along with recitations of first and second clients in the preamble. The claim also recites the capability of encryption by taking a private key and computing a cryptographic signature. In reviewing the written disclosure at paragraphs 52-53, 106 and 113 the memory and network interface are described in a manner that includes no technological improvement to the functioning of the memory and network interface and only describes

a particular technological environment for which an intermediary described in paragraph 113 as a "facilitator" is linked. With regard to the encryption capabilities no particular algorithm for computing a signature is described in the written disclosure beyond the recitations at pages 17, 18 and 28 that in order to consummate a transaction that a plurality of signatures are required and the function is described at a generally high level by the written disclosure such that in the broadest reasonable interpretation the claim scope encompasses encryption that could be performed by human beings. Even if a computer calculation of the signature were inferred from the claim the written disclosure relies on prior art signature calculation mechanisms such as multisignature transactions (see footnote 2 of page 4 of the written disclosure) or P2SH (97 and 104 of the written disclosure) and therefore do not constitute any technological improvement to the functioning of the computer itself. With regard to the two clients paragraph 110 in describing the client also describes a generic computing device with no technological improvement. The transfer mechanism per paragraphs 53, 54 and 96 are not elements of physical structure but instead are protocols involving at least decentralized currency ("Where a decentralized digital currency [e.g., the Bitcoin protocol, the Ethereum protocol, or similar] *is used as the transfer mechanism*...", 96) but per paragraph 49 can also involve centralized currency and the broadest reasonable interpretation of the term transfer mechanism can be viewed as any form of monetary exchange scheme. No technological improvement is recited in the claim nor does the combination of memories, network interfaces, transfer mechanism and two clients serve to form an ordered combination of elements that results in any technological improvement. It is abundantly clear that the claim does not involve any ordered combination of elements

as the recited transfer mechanism along with the two clients do not utilize any special properties of a network or distributed computing in order to gain any technological improvement and merely are directed towards a centralized, "one-size-fits-all" technological implementation and the clients merely serve as representatives of human counterparts engaging in a contract (*BASCOM Glob. Internet Servs. v. AT&T Mobility, LLC*, 119 USPQ2d 1236 (Fed. Cir. 2016)). It is also clear that no similarity is present with regard to *McRO* (*McRO, Inc. v. Bandai Namco Games Am. Inc.*, 120 USPQ2d 1091 (Fed. Cir. 2016)) as the process applied in McRO which involved the evaluation of a plurality of subsequences of phonemes in order to set morph weights and was a process that was not previously used by human beings in performing lip synchronization between the animated characters and the reproduced sounds. While *McRO* acknowledged that human beings could perform the operations recited in the steps it was also clear that human beings had never previously acted in such a manner, particularly as it applied to the evaluation of subsequences of phonemes in order to set the morph weights. However in the instant claims the recited operations of transferring payments and utilizing trusted intermediaries in making a payment as part of a contractual relationship are all operations that have previously been done by human beings in the same manner being claimed. It is also clear that there is no similarity to *DDR Holdings* (*DDR Holdings, LLC v. Hotels.com, LP*, 113 USPQ2d 1097 (Fed. Cir. 2014)) as there is nothing in the claims themselves or even in the written description to explicitly state or even implicitly suggest that the claims involve anything more than generic computer operations. It is also clear that there is no similarity to *Enfish* (*Enfish, LLC v. Microsoft Corp.*, 118 USPQ2d 1684 (Fed. Cir. 2016)) because nothing within the

claim or the four corners of the written description provides any teaching or suggestion of an improved computer algorithm for analyzing data such as the self-referential table of *Enfish* that brings about an improvement to the computer itself where *Enfish* taught that the claimed invention brought about "increased flexibility, faster search times, and smaller memory requirements" (*Enfish* at 1690). There is also no technological improvement being made to any external technology (*Diamond v. Diehr*, 450 U.S. 175, 184 (1981)). The written disclosure at paragraphs 52-53, 106, 110 and 113 describe only the use of a generic unimproved computing environment and describes the elements in a manner that indicates that the additional elements are sufficiently well-known that the specification does not need to describe the particulars of such additional elements to satisfy 35 U.S.C. §112 (a) and the disclosure itself recites at paragraph 108 that "The invention pertains to agreements among distinct parties that contemplate transfer of title to property, as well as any industry where that may be of value or importance" and clearly falls within the grouping of commercial/legal interactions under the groupings. ("In other words, the claims in *Diehr* were patent eligible because they improved an existing technological process, not because they were implemented on a computer", *Alice* at 1983). Therefore it is clear that no inventive concept is present sufficient to confer eligibility in light of the fact that the claims are clearly directed towards an abstract idea. Therefore claims 24, 26 and 28-29 are rejected under 35 U.S.C. § 101 as being directed towards ineligible subject matter.

Claim Rejections - 35 USC § 112

14. 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.

15. Claims 1, 3-6 and 9 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.

16. Claim 1 recites a device and recites that the device comprises a first memory, a first network interface and a first computer processor and continues by reciting operations describing the functions performed by the first memory, first network interface and first computer processor. It is clear from the claim that the operations attributed to the device end with the final limitation "publish the inchoate disbursement transaction record to at least one of the first client and the second client". However the claim goes on to claim both a first client and a second client and describe the structure comprising the first client and second client. It is also clear that the device as claimed does not encompass the first client or the second client as the device is claimed as performing operations that show a clear line of separation between the device and the first and second client as evidenced by the final limitation of "publish the inchoate disbursement transaction record to at least one of the first client and the second client". Therefore the claim is unclear as the claim is purportedly directed towards only the device however the claim is claiming operations being performed on the first and second client along with reciting the structure comprising the first and second client. As the first and second clients are divorced from the structure of the claimed device it is unclear whether infringement would take place only through possession of the claimed

device or requires the possession of each of the device, first client and second client (*In re Katz Interactive Call Processing Patent Litigation*, 639 F.3d 1303, 97 USPQ2d 1737 (Fed. Cir. 2011), *Rembrandt Data Techs., LP v. AOL, LLC*, 641 F.3d 1331, 98 USPQ2d 1393 (Fed. Cir. 2011), *UltimatePointer, L.L.C. v. Nintendo Co.*, 816 F.3d 816, 118 USPQ2d 1125 (Fed. Cir. 2016), *MasterMine Software, Inc. v. Microsoft Corp.*, 124 USPQ2d 1618 (Fed. Cir. 2017)).

17. Claims 3-6 and 9 are also rejected as being dependent upon claim 1.

Claim Rejections - 35 USC § 103

18. 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.

19. Claims 1, 3-6, 9, 12, 15-17, 20, 23-24, 26, 28, 29 and 31 are rejected under 35 U.S.C. 103 as being unpatentable over Rosen (U.S. Patent Publication 2003/0070080) in view of Feigelson (U.S. Patent Publication 2013/0166455).

20. As per claim 1

Rosen discloses a device for facilitating a value transfer between a first party utilizing a first client and a second party utilizing a second client via a transfer mechanism (0026, 0149-0151, 0161 "The Pay/Exchange application 35 supervises the sending and receiving of electronic notes 11 between Transaction money modules 4", Figure 56)

Rosen discloses a first memory comprising a transaction record sector and a first key pair sector for storing a first asymmetric key pair, the first asymmetric key pair comprising a first private key and a first public key (0162 "The Tran Log Mgr. application 36 provides the management and overseeing of a log that records completed transactions undertaken by the money module", 0189-0190, 0685-0688 "Each primary trusted server 210 has its own public key and corresponding private key", claim 1, claim 2, claim 13)

Rosen discloses a first network interface for receiving terms (0231-0234)

Rosen discloses the terms comprising at least one of a first principal amount or a second principal amount (0165)

Rosen discloses a reference to at least one of a first data source or a second data source (0159, 1297)

Rosen discloses an expiration timestamp (Figure 51 in element 1027, 0118, 0261, 0274, 0281) (Examiner notes that the term "expiration timestamp" appears to only be limited to a time at which something expires as a timestamp in typical usage reflects current time, not a past or future time)

Rosen discloses a first computer processor coupled to the first memory and the first network interface, the first computer processor configured to: compute one or more disbursement amounts by applying a disbursement function to: at least one of the first principal amount or the second principal amount and the value from at least one of the first data source or the second data source (0157-0174, 0176-0179, 0184, 0535, 0798-0802)

Rosen discloses read the first private key from the first key pair sector (0504, claim 13)

Rosen discloses compute a first cryptographic signature from the first private key (0660, 0662, 0702)

Rosen discloses create an inchoate disbursement transaction record comprising: a commit input for receiving a commit amount from a commit transaction (0157, 0546, 1941)

Rosen discloses one or more disbursement amounts comprising the disbursement amounts (0157-0174, 0176-0179, 0184, 0535, 0798-0802)

Rosen discloses the first cryptographic signature (1946)

Rosen discloses publish the inchoate disbursement transaction record to at least one of the first client and the second client (0142-0143, 0588-0591, Figure 3, Figure 7, Figure 36A)

Rosen discloses where the first client comprises: a second memory comprising a second key pair sector for storing a second asymmetric key pair, the second asymmetric key pair comprising a second private key and a second public key (0142-0143, 0159, 0191, 0662, 0749, claim 91)

Rosen discloses a second network interface (0666)

Rosen discloses a second computer processor coupled to the second memory and the second network interface, the second computer processor configured to read the second private key from the second key pair sector (0630, 0664, 0749, Figure 52)

Rosen discloses read the inchoate disbursement transaction; compute a second cryptographic signature from the second private key; create a complete disbursement

transaction record comprising: the commit input; the disbursement outputs; the first cryptographic signature; and the second cryptographic signature; and create a disbursement transaction by submitting the complete disbursement transaction record to the transfer mechanism (0157-0174, 0176-0179, 0288, 0504, 0535, 0546, 0791-0802)

Rosen discloses where the second client comprises a third memory comprising a third key pair sector for storing a third asymmetric key pair, the third asymmetric key pair comprising a third private key and a third public key (1660-1663, Figure 57A)

Rosen discloses a third network interface (0670)

Rosen discloses a third computer processor coupled to the third memory and the third network interface, the third computer processor configured to read the third private key from the third key pair sector (0664, 1660-1663, Figure 56)

Rosen, while disclosing electronic money (Abstract), does not explicitly disclose wherein the transfer mechanism comprises a decentralized currency. Feigelson teaches wherein the transfer mechanism comprises a decentralized currency (0050-0051)

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the electronic monetary system of Rosen with the creation and use of digital currency of Feigelson for the purpose of maintaining secrecy of information in order to control its value (0003).

21. As per claim 3

Rosen discloses where: the first computer processor is further configured to compute the one or more disbursement amounts by applying the disbursement function to: the first principal amount; and the value from the first data source (0157-0174)

22. As per claim 4

Rosen discloses where the first computer processor is further configured to: compute a third cryptographic signature from the first private key; create an inchoate refund transaction record comprising: a commit input for receiving the commit amount from the commit transaction: a refund output comprising a refund amount; the third cryptographic signature; and a lock time; and publish the inchoate refund transaction record to at least one of the first client or the second client (0157-0174, 0176-0179, 0251, 0300, 0806-0807, 0845)

23. As per claim 5

Rosen discloses where: the first key pair sector further stores a fourth asymmetric key pair, the fourth asymmetric key pair comprising a fourth private key and a fourth public key; and the first computer processor is further configured to: read the fourth private key from the first key pair sector; compute a third cryptographic signature from the fourth private key; create a commit transaction record, the commit transaction record comprising: a first principal input for receiving the first principal amount from a first principal transaction; a commit output comprising the commit amount; the third cryptographic signature; and create the commit transaction by submitting the commit transaction record to the transfer mechanism (0177, 0193, 0546, 0662, 0791-0802, claims 1, 2 and 13)

24. As per claim 6

Rosen discloses where the first asymmetric key pair consists of the fourth asymmetric key pair, the first private key consists of the fourth private key, and the first public key consists of the fourth public key (0193, 0683-0688, 0854, Figure 56, claim 13)

25. As per claim 9

Rosen discloses where: the reference to the first data source comprises at least one of a reference to a base instrument and a reference to a quote instrument; and the first computer processor is further configured to compute the disbursement amounts on or after the expiration timestamp (0118, 0180, 0278, 0284, 0535-0540, 0628)

26. As per claim 12

Rosen discloses a device for facilitating a value transfer between a first party utilizing a first client and a second party utilizing a second client via a transfer mechanism (0026, 0149-0151, 0161 "The Pay/Exchange application 35 supervises the sending and receiving of electronic notes 11 between Transaction money modules 4", Figure 56)

Rosen discloses a first memory comprising a transaction record sector and a first key pair sector for storing a first asymmetric key pair, the first asymmetric key pair comprising a first private key and a first public key (0162 "The Tran Log Mgr. application 36 provides the management and overseeing of a log that records completed transactions undertaken by the money module", 0189-0190, 0685-0688 "Each primary trusted server 210 has its own public key and corresponding private key", claim 1, claim 2, claim 13)

Rosen discloses a first network interface for receiving terms (0231-0234)

Rosen discloses the terms comprising at least one of a first principal amount or a second principal amount (0165)

Rosen discloses a reference at least one of a first data source or a second data source (0159, 1297)

Rosen discloses an expiration timestamp (Figure 51 in element 1027, 0118, 0261, 0274, 0281) (Examiner notes that the term “expiration timestamp” appears to only be limited to a time at which something expires as a timestamp in typical usage reflects current time, not a past or future time)

Rosen discloses a first computer processor coupled to the first memory and the first network interface, the first computer processor configured to: compute one or more disbursement amounts by applying a disbursement function to: at least one of the first principal amount or the second principal amount and the value from at least one of the first data source or the second data source (0157-0174, 0176-0179, 0184, 0535, 0798-0802)

Rosen discloses read the first private key from the first key pair sector (0504, claim 13)

Rosen discloses compute a first cryptographic signature from the first private key (0660, 0662, 0702)

Rosen discloses create an inchoate disbursement transaction record comprising: a commit input for receiving a commit amount from a commit transaction (0157, 0546, 1941)

Rosen discloses one or more disbursement amounts comprising the disbursement amounts (0157-0174, 0176-0179, 0184, 0535, 0798-0802)

Rosen discloses the first cryptographic signature (1946)

Rosen discloses publish the inchoate disbursement transaction record to at least one of the first client and the second client (0142-0143, 0588-0591, Figure 3, Figure 7, Figure 36A)

Rosen discloses where the first client comprises: a second memory comprising a second key pair sector for storing a second asymmetric key pair, the second asymmetric key pair comprising a second private key and a second public key (0142-0143, 0159, 0191, 0662, 0749, claim 91)

Rosen discloses a second network interface (0666)

Rosen discloses a second computer processor coupled to the second memory and the second network interface, the second computer processor configured to read the second private key from the second key pair sector (0630, 0664, 0749, Figure 52)

Rosen discloses read the inchoate disbursement transaction; compute a second cryptographic signature from the second private key; create a complete disbursement transaction record comprising: the commit input; the disbursement outputs; the first cryptographic signature; and the second cryptographic signature; and create a disbursement transaction by submitting the complete disbursement transaction record to the transfer mechanism (0157-0174, 0176-0179, 0288, 0504, 0535, 0546, 0791-0802)

Rosen discloses where the second client comprises a third memory comprising a third key pair sector for storing a third asymmetric key pair, the third asymmetric key pair comprising a third private key and a third public key (1660-1663, Figure 57A)

Rosen discloses a third network interface (0670)

Rosen discloses a third computer processor coupled to the third memory and the third network interface, the third computer processor configured to read the third private key from the third key pair sector (0664, 1660-1663, Figure 56)

Rosen, while disclosing electronic money (Abstract), does not explicitly disclose wherein the transfer mechanism comprises a decentralized currency. Feigelson teaches wherein the transfer mechanism comprises a decentralized currency (0050-0051)

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the electronic monetary system of Rosen with the creation and use of digital currency of Feigelson for the purpose of maintaining secrecy of information in order to control its value (0003).

27. As per claim 15

Rosen discloses where the first computer processor is further configured to: compute a third cryptographic signature from the first private key; create an inchoate refund transaction record comprising: a commit input for receiving the commit amount from the commit transaction; a refund output comprising a refund amount; and iii. the third cryptographic signature; and publish the inchoate refund transaction record to at least one of the first client and the second client. (0176-0179, 0251, 0300, 0806-0807)

28. As per claim 16

Rosen discloses where: the first key pair sector further stores a fourth asymmetric key pair, the fourth asymmetric key pair comprising a fourth private key and a fourth public key; the first computer processor is further configured to: compute one or more disbursement amounts by applying the disbursement function to: the first principal

amount; and the value from the first data source; read the fourth private key from the first key pair sector; compute a third cryptographic signature from the fourth private key; iv. create a commit transaction record comprising: a first principal input for receiving the first principal amount from a first principal transaction; a commit output comprising the commit amount; and the third cryptographic signature; and create the commit transaction by submitting the commit transaction record to the transfer mechanism (0157-0174, 0177, 0193, 0546, 0662, 0791-0802, claims 1, 2 and 13)

29. As per claim 17

Rosen discloses where the second computer processor is configured to: compute a fourth cryptographic signature from the second private key; create a first principal transaction record comprising: a first principal output comprising the first principal amount; and the fourth cryptographic signature; and create the first principal transaction by submitting the first principal transaction record to the transfer mechanism (0157-0174, 0176-0179, 0300, 0791-0802)

30. As per claim 20

Rosen discloses where: the reference to at least one of the first data source or the second data source comprises at least one of a reference to a base instrument or a reference to a quote instrument; and the first computer processor is further configured to compute the disbursement amounts on or after the expiration timestamp (0118, 0180, 0278, 0284, 0535-0540, 0628)

31. As per claim 23

Rosen discloses where: the second computer processor is further configured to: compute a third cryptographic signature from the second private key; create a first

principal transaction record comprising: a first principal output comprising the first principal amount; and the third cryptographic signature; and create a first principal transaction by submitting the first principal transaction record to the transfer mechanism; and the third computer processor is further configured to: compute a fourth cryptographic signature from the third private key; create a second principal transaction record comprising: a second principal output comprising the second principal amount; and the fourth cryptographic signature; and create a second principal transaction by submitting the second principal transaction record to the transfer mechanism (0157-0174, 0176-0179, 0300, 0490, 0662, 0791-0802)

32. As per claim 24

Rosen discloses a method for facilitating value transfers between a first party utilizing a first client and a second party utilizing a second client via a transfer mechanism (Abstract, 0149-0151, 0161, Figure 56)

Rosen discloses the transfer mechanism comprising a digital currency (0118)

Rosen discloses the method comprising: storing a first asymmetric key pair in a first key pair sector of a first memory, the first asymmetric key pair comprising a first private key and a first public key (0162, 0189-0190, 0685-688, claims 1, 2 and 13)

Rosen discloses storing a second asymmetric key pair in a second key pair sector of a second memory, the second asymmetric key pair comprising a second private key and a second public key (0142-0143, 0159, 0749, claim 91)

Rosen discloses storing a third asymmetric key pair in the second key pair sector, the third key pair comprising a third private key and a third public key (1660-1663, Figure 57A)

Rosen discloses storing a fourth asymmetric key pair in a third key pair sector of a third memory, the fourth asymmetric key pair comprising a fourth private key and a fourth public key (0193, 0683-0688, 0854, Figure 56, claim 13)

Rosen discloses transmitting terms from one of the first or second client via a first network interface (0231-0234) the terms comprising: at least one of a first principal amount or a second principal amount (0165) and a reference to at least one of a first data source or a second data source (0159, 1297) and an expiration timestamp (Figure 51 in element 1027, 0118, 0261, 0274, 0281) (Examiner notes that the term “expiration timestamp” appears to only be limited to a time at which something expires as a timestamp in typical usage reflects current time, not a past or future time)

Rosen discloses receiving the terms at a facilitator via a second network interface (0026, 0589, 0666)

Rosen discloses computing one or more disbursement amounts by applying a disbursement function to: at least one of the first principal amount or the second principal amount and the value from at least one of the first data source or the second data source (0157-0174, 0176-0179, 0184, 0535, 0798-0802)

Rosen discloses reading the first private key from the first key pair sector (0504, claim 13)

Rosen discloses computing a first cryptographic signature from the first private key (0660, 0662, 0702)

Rosen discloses creating a first principal transaction record comprising: a first principal output comprising the first principal amount; and the first cryptographic signature (0157-0174)

Rosen discloses creating a first principal transaction by submitting the first principal transaction record to the transfer mechanism (0546, 0791-0802)

Rosen discloses reading the second private key from the second key pair sector (0630, 0664, 0749, Figure 52)

Rosen discloses computing a second cryptographic signature from the second private key (0660, 0662)

Rosen discloses creating a commit transaction record comprising: a first principal input for receiving the first principal amount from the first principal transaction; a commit output comprising a commit amount; and iii. the second cryptographic signature (0157-0174, 0176-0179, 0300, 0535, 0791-0802)

Rosen discloses creating the commit transaction by submitting the commit transaction record to the transfer mechanism (0157-0174, 0176-0179, 0300, 0535, 0791-0802)

Rosen discloses retrieving a value from the first data source (0149, 0677)

Rosen discloses reading the third private key from the second key pair sector (0664, 1660-1663, Figure 56)

Rosen discloses computing a third cryptographic signature from the second private key (0157-0174, 0176-0179, 0193, 0300, 0791-0802)

Rosen discloses creating an inchoate disbursement transaction record comprising: a commit input for receiving a commit amount from a commit transaction (0157-0174, 0176-0179, 0193, 0300, 0791-0802)

Rosen discloses one or more disbursement outputs comprising the one or more disbursement amounts (0157-0174, 0176-0179, 0184, 0535, 0798-0802)

Rosen discloses the third cryptographic signature (0157-0174, 0176-0179, 0193, 0300, 0791-0802)

Rosen discloses publishing the inchoate disbursement transaction record (0157-0174, 0176-0179, 0193, 0300, 0791-0802)

Rosen discloses reading the inchoate disbursement transaction record (0157-0174, 0176-0179, 0193, 0300, 0660, 0662, 0791-0802)

Rosen discloses reading the fourth private key from the third key pair sector (0157-0174, 0176-0179, 0193, 0300, 0660, 0662, 0791-0802)

Rosen discloses computing a fourth cryptographic signature from the fourth private key (0157-0174, 0176-0179, 0193, 0300, 0660, 0662, 0791-0802)

Rosen discloses creating a complete disbursement transaction record comprising: the commit input; the one or more disbursement amounts; the third cryptographic signature; and the fourth cryptographic signature (0157-0174, 0176-0179, 0193, 0300, 0660, 0662, 0791-0802)

Rosen discloses creating a disbursement transaction by submitting the complete disbursement transaction record to the transfer mechanism (0157-0174, 0176-0179, 0193, 0300, 0660, 0662, 0791-0802)

Rosen, while disclosing electronic money (Abstract), does not explicitly disclose wherein the transfer mechanism comprises a decentralized currency. Feigelson teaches wherein the transfer mechanism comprises a decentralized currency (0050-0051)

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the electronic monetary system of Rosen with the creation and use

of digital currency of Feigelson for the purpose of maintaining secrecy of information in order to control its value (0003).

33. As per claim 26

Rosen discloses computing a fifth cryptographic signature from the third private key; creating an inchoate refund transaction record comprising: a commit input for receiving the commit amount from the commit transaction; a refund output comprising a refund amount; the fifth cryptographic signature; and a lock time; and publishing the inchoate refund transaction record (0157-0174, 0176-0179, 0251, 0300, 0660, 0662, 0806-0807, 0845)

34. As per claim 28

Rosen discloses storing a fifth asymmetric key pair in a fourth key pair sector of a fourth memory, the fifth asymmetric key pair comprising a fifth private key and a fifth public key; reading the fifth private key from the fourth key pair sector; computing a fifth cryptographic signature from the fifth private key; creating a second principal transaction record comprising: a second principal output comprising the second principal amount; and the fifth cryptographic signature; creating a second principal transaction by submitting the second principal transaction record to the transfer mechanism; computing one or more disbursement amounts by applying a disbursement function to: the value from the first data source; and at least one of: the first principal amount; and the second principal amount (0157-0174, 0176-0179, 0288, 0504, 0535, 0546, 0791-0802)

35. As per claim 29

Rosen discloses computing a sixth cryptographic signature from the third private key; creating an inchoate refund transaction record comprising: a commit input for receiving the commit amount from the commit transaction; one or more refund outputs comprising one or more refund amounts; the sixth cryptographic signature; and a lock time; and publishing the inchoate refund transaction record (0157-0174, 0176-0179, 0251, 0300, 0660, 0662, 0806-0807, 0845)

36. As per claim 31

Rosen discloses wherein the one or more disbursement output further comprise one or more conditions requiring approval of at least one of the first party or the second party, and the one or more conditions include a condition to determine if a sum of the one or more disbursement amounts is equal or less than the commit amount from the commit transaction (Figure 30 element 704, Figure 30A element 718, Figure 36 element 822, 0045, 0531-0532, 0589-0591, 1022)

Conclusion

37. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JAMES D NIGH whose telephone number is (571)270-5486. The examiner can normally be reached on 5 to 7:15 AM and 10:45 AM to 4:30 PM.

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, Neha Patel can be reached on (571) 270-1492. 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.

/JAMES D NIGH/
Senior Examiner, Art Unit 3685

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/309,612	Middleton et al.
	Examiner	Art Unit
	JAMES D NIGH	3685

CPC - Searched*		
Symbol	Date	Examiner

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
EAST Text Search	07/18/2019	JDN
EAST Text Search	06/05/2020	JDN

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

	/JAMES D NIGH/ Primary Examiner, Art Unit 3685

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	5	("20030070080" | "20130054471" | "20130166455" | "20130179337" | "20130212388").PN.	US-PGPUB; USPAT	AND	ON	2019/07/18 07:53
S2	17	(server near20 ("public key") near20 ("private key")) ((transaction or principal) near10 amount) (signature near20 "private key") ((client or agent) near20 "private key") ((digital or electronic) near10 currency) @ad<="20140509"	US-PGPUB; USPAT	AND	ON	2019/07/18 08:22
S3	2	("20170187535").PN.	US-PGPUB; USPAT; USOCR; DERWENT	AND	ON	2019/12/09 12:05
S4	17	((intermediary OR server) near20 ("public key") near20 ("private key")) ((transaction or principal) near10 amount) (signature near20 "private key") ((client or agent) near20 "private key") ((digital or electronic) near10 currency) @ad<="20140509"	US-PGPUB; USPAT	AND	ON	2020/06/01 12:40
S5	17	((intermediary OR server) near20 ("public key") near20 ("private key")) ((transaction or principal) near10 amount) (signature near20 "private key") ((client or agent) near20 "private key") ((digital or electronic) near10 currency) (@ad<="20140509" OR @pd<="20140509" @rlad<="20140509" OR @prad<="20140509") NOT ("continuation-in-part" AND @ad>"20140509")	US-PGPUB; USPAT	AND	ON	2020/06/01 12:41

6/5/2020 8:38:32 AM
C:\Users\jnigh\Documents\EAST\Workspaces\15309612.wsp

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.
15/309,612	11/08/2016	Reginald Middleton	4675.1002BS	2321

86636 7590 09/17/2020
BRUNDIDGE & STANGER, P.C.
1925 BALLENGER AVENUE, STE. 560
ALEXANDRIA, VA 22314

EXAMINER	
NIGH, JAMES D	

ART UNIT	PAPER NUMBER
3685	

MAIL DATE	DELIVERY MODE
09/17/2020	PAPER

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.

Applicant-Initiated Interview Summary	Application No. 15/309,612	Applicant(s) Middleton et al.	
	Examiner JAMES D NIGH	Art Unit 3685	AIA (FITF) Status Yes

All participants (applicant, applicants representative, PTO personnel):

(1) JAMES D. NIGH.

(2) Misung Lee (Reg. No. 78,307).

(3) Reginald Middleton (Inventor).

(4) Matthew Bogosian (Inventor).

Date of Interview: 15 September 2020.

Type: ☑ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☑ No.
If Yes, brief description: _____.

Issues Discussed ☑101 ☐112 ☐102 ☑103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: 24.

Identification of prior art discussed: cited prior art.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Discussed 101 rejection, particularly in light of the 2019 Patent Subject Matter Eligibility Guidance and contrasted the instant claim with the examples in the guidance. Some discussion was held with regard to redrafting the claim to involve less of a financial nature. No agreement was reached. With regard to the 103 rejection there was some discussion regarding the nature of the facilitator and in particular that the facilitator was decentralized. Examiner still views some of the aspects of the facilitator as being that of an intermediary, but also indicated that if the claim is being redrafted in order to overcome 101 that the prior art would also need to be reevaluated based on whatever new construction is placed into the claims. No agreement was reached..

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☑ Attachment

/JAMES D NIGH/
Senior Examiner, Art Unit 3685

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiners responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicants correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:
1) A brief description of the nature of any exhibit shown or any demonstration conducted,-
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
(The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicants record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiners version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, Interview Record OK on the paper recording the substance of the interview along with the date and the examiners initials.

Applicant Initiated Interview Request Form

Application No.: 15/309,612 First Named Applicant: Reginald Middleton
Examiner: NIGH, JAMES D Art Unit: 3685 Status of Application: NON-FINAL

Tentative Participants:
(1) Examiner Nigh (2) Misung Lee

(3) Reginald Middleton (4) Matthew Bogosian

Proposed Date of Interview: September 15, 2020 **Proposed Time:** 1:00 PM (ET) **(AM/PM)**

Type of Interview Requested:
(1) [✓] Telephonic (2) [ ] Personal (3) [ ] Video Conference

Exhibit To Be Shown or Demonstrated: [ ] YES [✓] NO
If yes, provide brief description: _____

Issues To Be Discussed

Issues (Rej., Obj., etc)	Claims/ Fig. #s	Prior Art	Discussed	Agreed	Not Agreed
(1) 35 U.S.C. § 101	Claim 24		[ ]	[ ]	[ ]
(2) 35 U.S.C. § 103	Claim 24		[ ]	[ ]	[ ]
(3)			[ ]	[ ]	[ ]
(4)			[ ]	[ ]	[ ]

[ ] Continuation Sheet Attached [ ] Proposed Amendment or Arguments Attached
Brief Description of Arguments to be Presented: _____

An interview was conducted on the above-identified application on _____

NOTE: This form should be completed and filed by applicant in advance of the interview (see MPEP § 713.01). If this form is signed by a registered practitioner not of record, the Office will accept this as an indication that he or she is authorized to conduct an interview on behalf of the principal (37 CFR 1.32(a)(3)) pursuant to 37 CFR 1.34. This is not a power of attorney to any above named practitioner. See the Instruction Sheet for this form, which is incorporated by reference. By signing this form, applicant or practitioner is certifying that he or she has read the Instruction Sheet. After the interview is conducted, applicant is advised to file a statement of the substance of this interview (37 CFR 1.133(b)) as soon as possible. This application will not be delayed from issue because of applicant's failure to submit a written record of this interview.

/Misung Lee/
Applicant/Applicant's Representative Signature

Examiner/SPE Signature

Misung Lee
Typed/Printed Name of Applicant or Representative

78,307
Registration Number, if applicable

This collection of information is required by 37 CFR 1.133. 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 24 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.

PTOL-413A (08-10)
Approved for use through 07/31/2012. 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.

Instruction Sheet for:
APPLICANT INITIATED INTERVIEW REQUEST FORM

(Not to be Submitted to the USPTO)

1. If this form is signed by a registered practitioner not of record, the authority to submit the Applicant Initiated Interview Request Form is pursuant to limited authority to act in a representative capacity under 37 CFR 1.34 and further proof of authority to act in a representative capacity may be required. *See* 37 CFR 1.34.

   The Office will accept the signed form as an indication that the registered practitioner not of record is authorized to conduct an interview on behalf of the principal in pursuant to 37 CFR 1.34.

   For more information, see the "Conducting an Interview with a Registered Practitioner Acting in a Representative Capacity" notice which is available on the USPTO Web site at: http://www.uspto.gov/patents/law/notices/2010.jsp.

2. This is not a power of attorney to any named practitioner. Accordingly, any registered practitioner not of record named on the form does not have authority to sign a request to change the correspondence address, a request for express abandonment, a disclaimer, a power of attorney, or other document requiring the signature of the applicant, assignee of the entire interest or an attorney of record. If appropriate, a separate power of attorney to the named practitioner should be executed and filed in the US Patent and Trademark Office.

3. Any interview concerning an unpublished application under 35 U.S.C. § 122(b) with a registered practitioner not of record, pursuant to 37 CFR 1.34, will be conducted based on the information and files supplied by the practitioner in view of the confidentiality requirements of 35 U.S.C. § 122(a).

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.

Application Serial No. 15/309,612
Filing Date ..... November 08, 2016
Confirmation No. 2321
Inventorship ..... Reginald Middleton
Group Art Unit 3685
Examiner ..... NIGH, JAMES D
Attorney Docket No. 4675.1002BS
Title: ..... DEVICES, SYSTEMS, AND METHODS FOR FACILITATING LOW TRUST AND ZERO TRUST VALUE TRANSFERS

To: Examiner Nigh

From: Misung Lee (T. 703-718-4018)
Brundidge & Stanger, PC
1925 Ballenger Avenue, Suite 560
Alexandria, VA 22314

Examiner Nigh:

Please consider the following in anticipation of our conversation during an interview.

FOR DISCUSSION PURPOSE ONLY

35 U.S.C. § 101

Applicant's representative would like to discuss regarding proposed amendments of Claim 24 as below (emphasis added):

> A method for ***facilitating value transfers between a first party utilizing a first client and a second party utilizing a second client via a transfer mechanism, the transfer mechanism comprising a decentralized digital currency that is accessible via a computer network by the device, the first client, and the second client, respectively***, the method comprising:
>
> storing a first asymmetric key pair in a first key pair sector of a first memory, the first asymmetric key pair comprising a first private key and a first public key;
>
> storing a second asymmetric key pair in a second key pair sector of a second memory, the second asymmetric key pair comprising a second private key and a second public key;
>
> storing a third asymmetric key pair in the second key pair sector, the third key pair comprising a third private key and a third public key;
>
> storing a fourth asymmetric key pair in a third key pair sector of a third memory, the fourth asymmetric key pair comprising a fourth private key and a fourth public key;
>
> transmitting terms from one of the first or second client via a first network interface, the terms comprising:

at least one of a first principal amount or a second principal amount;

a reference to at least one of a first data source or a second data source; and

an expiration timestamp;

receiving the terms at a facilitator via a second network interface;

computing one or more disbursement amounts by applying a disbursement function to:

at least one of the first principal amount or the second principal amount, and

a value from at least one of the first data source or the second data source;

reading the first private key from the first key pair sector;

computing a first cryptographic signature from the first private key;

creating a first principal transaction record comprising:

a first principal output comprising the first principal amount; and

the first cryptographic signature;

creating a first principal transaction by submitting the first principal transaction record to the transfer mechanism;

reading the second private key from the second key pair sector;

computing a second cryptographic signature from the second private key;

creating a commit transaction record comprising:

a first principal input for receiving the first principal amount from the first principal transaction;

a commit output comprising a commit amount; and

the second cryptographic signature;

creating the commit transaction by submitting the commit transaction record to the transfer mechanism;

retrieving a value from the first data source;

reading the third private key from the second key pair sector;

computing a third cryptographic signature from the second private key;

creating an inchoate disbursement transaction record comprising:

a commit input for receiving a commit amount from a commit transaction;

one or more disbursement outputs comprising the one or more disbursement amounts; and

the third cryptographic signature;

publishing the inchoate disbursement transaction record;

reading the inchoate disbursement transaction record;

reading the fourth private key from the third key pair sector;

computing a fourth cryptographic signature from the fourth private key;

creating a complete disbursement transaction record comprising:

the commit input;
the one or more disbursement outputs;
the third cryptographic signature; and
the fourth cryptographic signature;

creating a disbursement transaction by submitting the complete disbursement transaction record to the transfer mechanism; and

broadcasting, via the transfer mechanism comprising the decentralized digital currency, the complete disbursement transaction record to the facilitator, the first client, and the second client for verifying and effecting the disbursement transaction.

The claimed combination improves a value transfer technology, particularly, a value transfer via a transfer mechanism comprising a decentralized digital currency with enhanced security and mitigated third party risks. At least the above emphasized features of amended Claim 24, for example, permits providing enhanced security for either party entering into the value transfer via the decentralized digital currency of the transfer mechanism, without requiring expensive tamper-proof electronic units, because the decentralized digital currency of the transfer mechanism requires that transactions are validated by a number of individuals before the transaction actually occurs and is recorded on the ledger (see paragraphs [0010] and [0011] of the U.S. Patent Application Publication).

Furthermore, implementing specific improvements achieved by the present application would not be possible using conventional transfer mechanisms which all involve third party intermediaries who temporarily control disposition of transfers. That is, the present application implemented on the decentralized digital currencies affords transactions between parties where no intermediary has an opportunity to behave badly or incompetently (see paragraphs [0009], [0015], [0016], and [0018] of the U.S. Patent Application Publication).

35 U.S.C. § 103

It is respectfully submitted that the proposed combination of the cited references fails to teach or suggest above recitation of Claim 24.

In contrast to the allegations that the facilitator as claimed "clearly is playing a centralized role," as alleged by the Office Action (at pages 3-4), the facilitator as recited in Claim 24 participates in the value transfer but the facilitator alone does not control disposition. The claimed decentralized digital currency prevents the facilitator from being commandeered to effect transfers not contemplated by at least one of the first or second clients. As such, by definition, the facilitator is a distributed participant that works in connection with the first and second clients, but that does not make it centralized. Further, not only Rosen fails to teach or suggest value transferring method implemented on decentralized digital currencies, but also *teaches away* the claimed method implemented on the decentralized digital currencies because Rosen identifies intermediaries who store and control currency (value) as agents or intermediaries or promissories (see Rosen, at paragraph [0026]). Furthermore, Feigelson does not compensate for the above deficiencies of Rosen, and it is also submitted that there is no motivation to one of ordinary skill in the art to combine Rosen and Feigelson.

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 15/309,612	Filing Date 11/08/2016	☐ 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 $80 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $420 =	
☐ 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	12/08/2020	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 18	Minus	** 30	= 0		x $100 =	0
	Independent (37 CFR 1.16(h))	* 3	Minus	*** 3	= 0		x $480 =	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.	ADMIN
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	/ERNEST D DAVIS/
*** 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

Application Serial No..... 15/309,612
Filing Date ..... November 08, 2016
Confirmation No. 2321
Inventorship ..... Reginald Middleton
Group Art Unit..... 3685
Examiner .....NIGH, JAMES D
Attorney Docket No. 4675.1002BS
Title:.....DEVICES, SYSTEMS, AND METHODS FOR FACILITATING LOW TRUST AND ZERO TRUST VALUE TRANSFERS

RESPONSE TO OFFICE ACTION OF JUNE 8, 2020 AND
STATEMENT OF SUBSTANCE OF INTERVIEW OF SEPTEMBER 15, 2020

To: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

From: Misung Lee
Customer No. 86636
Brundidge & Stanger, PC
1925 Ballenger Ave., Suite 560
Alexandria, VA 22314

Sir:

In response to the Non-Final Office Action dated June 8, 2020, for which the three-month shortened statutory period for response is extended to expire on December 8, 2020, and subsequent to the Examiner Interview conducted on September 15, 2020, the following amendments and remarks are respectfully submitted. Applicant also submits a Statement of Substance of Interview under 37 C.F.R. § 1.133(b). Favorable consideration is respectfully requested.

The Commissioner is hereby authorized to charge any deficiency of fees and credit any overpayments to Deposit Account Number 50-4888.

INTRODUCTORY COMMENTS

Statement of Substance of Interview begins on page 3.

The Listing of the Claims section begins on page 4.

Remarks section begins on page 19.

LISTING OF THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Claims pending:

- At time of the Action: **Claims 1, 3-6, 9, 12, 15-17, 20, 23, 24, 26, 28, 29 and 31**
- After this Reply: **Claims 1, 3-6, 9, 12, 15-17, 20, 23, 24, 26, 28, 29, 31, and 32**

Currently Canceled or Withdrawn Claims: **None**

Currently Amended Claims: **Claims 1, 3-6, 9, 12, 15-17, 20, 23, 24, 26, 28, 29 and 31**

New Claims: **Claim 32**

1. (**Currently Amended**) A computing device for ~~facilitating a value transfer~~ processing a transaction between ~~a first party utilizing~~ a first client device, and ~~a second party utilizing~~ a second client device via a transfer mechanism, the transfer mechanism comprising a decentralized digital currency, the computing device comprising:

a ~~first~~ memory ~~comprising a transaction record sector and a first key pair sector~~ for storing a first asymmetric key pair, the first asymmetric key pair comprising a first private key and a first public key;

a ~~first~~ network interface for receiving terms, the terms comprising:

at least one of a first principal ~~amount~~ data or a second principal ~~amount~~ data;

a reference to at least one of a first data source or a second data source; and

an expiration timestamp;

a ~~first~~ computer processor coupled to the ~~first~~ memory and the ~~first~~ network interface, the ~~first~~ computer processor configured to:

~~compute one or more disbursement amounts by applying a disbursement function to:~~

~~at least one of the first principal amount or the second principal amount, and~~

~~a value from at least one of the first data source or the second data source;~~

read the first private key from the ~~first key pair sector~~ memory;

compute a first cryptographic signature from the first private key;

create an inchoate ~~disbursement transaction~~ data record comprising:

a commit input for receiving a commit ~~amount~~ data from a commit transaction;

one or more ~~disbursement~~ output~~s~~ data ~~comprising~~ obtained from ~~the disbursement amounts~~ at least one of the first principal data or the second principal data, and a value data from at least one of the first data source or the second data source; and

the first cryptographic signature; and

publish the inchoate ~~disbursement transaction~~ data record to at least one of the first client device ~~and~~ or the second client device~~;~~,

wherein the inchoate data record is used by at least one of the first client device or the second client device to create a complete data record and to create a transaction by submitting the complete data record to the transfer mechanism,

wherein the transfer mechanism comprises the decentralized digital currency that is accessible via a computer network by the computing device, the first client device, and the second client device, respectively, and the complete data record is broadcast, via the transfer

mechanism to the computing device, the first client device, and the second client device for verifying and effecting the transaction,

wherein an external state is observed by each of the computing device, the first client device, and the second client device and the transaction is effected when an action by at least two of the computing device, the first client device, or the second client device is detected based on the observed external state.

~~where the first client comprises:~~

~~a second memory comprising a second key pair sector for storing a second asymmetric key pair, the second asymmetric key pair comprising a second private key and a second public key;~~

~~a second network interface; and~~

~~a second computer processor coupled to the second memory and the second network interface, the second computer processor configured to:~~

~~read the second private key from the second key pair sector;~~

~~read the inchoate disbursement transaction record;~~

~~compute a second cryptographic signature from the second private key;~~

~~create a complete disbursement transaction record comprising:~~

~~the commit input;~~

~~the disbursement outputs;~~

~~the first cryptographic signature; and~~

~~the second cryptographic signature; and~~

~~create a disbursement transaction by submitting the complete disbursement transaction record to the transfer mechanism; and~~

~~where the second client comprises;~~

~~a third memory comprising a third key pair sector for storing a third asymmetric key pair, the third asymmetric key pair comprising a third private key and a third public key;~~

~~a third network interface; and~~

~~a third computer processor coupled to the third memory and the third network interface, the third computer processor configured to read the third private key from the third key pair sector.~~

2. (**Canceled**)

3. (**Currently Amended**) The device of claim 1, where:

the ~~first~~ computer processor is configured to ~~compute~~ obtain the one or more ~~disbursement amounts~~ output data ~~by applying the disbursement function to:~~ based on:

the first principal ~~amount~~ data; and

the value data from the first data source.

4. (**Currently Amended**) The device of claim 1, where the ~~first~~ computer processor is further configured to:

compute a ~~third~~ second cryptographic signature from the first private key;

create an another inchoate ~~refund transaction~~ data record comprising:

a commit input for receiving the commit ~~amount~~ data from the commit transaction;

a refund output comprising a refund ~~amount~~ data;

the ~~third~~ second cryptographic signature; and

a lock time; and

publish the another inchoate ~~refund transaction~~ data record to at least one of the first client device or the second client device.

5. (**Currently Amended**) The device of claim 1, where:

the ~~first key pair sector~~ memory further stores a ~~fourth~~ second asymmetric key pair, the ~~fourth~~ second asymmetric key pair comprising a ~~fourth~~ second private key and a ~~fourth~~ second public key; and

the ~~first~~ computer processor is further configured to:

read the ~~fourth~~ second private key from the ~~first key pair sector~~ memory;

compute a third cryptographic signature from the ~~fourth~~ second private key;

create a commit transaction data record, the commit transaction data record comprising:

a first principal input for receiving the first principal ~~amount~~ data from a first principal transaction;

a commit output comprising the commit ~~amount~~data;

the third cryptographic signature; and

create the commit transaction by submitting the commit transaction data record to the transfer mechanism.

6. (**Currently Amended**) The device of claim 5, where the first asymmetric key pair consists of the ~~fourth~~ second asymmetric key pair, the first private key consists of the ~~fourth~~ second private key, and the first public key consists of the ~~fourth~~ second public key.

7. (**Canceled**)

8. (**Canceled**)

9. (**Currently Amended**) The device of claim1, where:

the reference to the first data source comprises at least one of a reference to a base instrument and a reference to a quote instrument; and

the ~~first~~ computer processor is further configured to compute the ~~disbursement amounts~~ output data on or after the expiration timestamp.

10. (**Canceled**)

11. (**Canceled**)

12. (**Currently Amended**) A system for ~~facilitating~~ processing a ~~value transfer~~ transaction between ~~a first party utilizing~~ a first client device and ~~a second party utilizing~~ a second client device via a transfer mechanism, ~~the transfer mechanism comprising a decentralized digital currency~~, the system comprising a ~~facilitator~~ computing device, the first client device, ~~and~~ the second client device, and the transfer mechanism;

the ~~facilitator~~ computing device comprising:

a first memory comprising ~~a transaction record sector and a first key pair sector~~ for storing a first asymmetric key pair, the first asymmetric key pair comprising a first private key and a first public key;

a first network interface for receiving terms, the terms comprising:

at least one of a first principal ~~amount~~ data or a second principal ~~amount~~ data;

a reference to at least one of a first data source or a second data source; and

an expiration timestamp; and

a first computer processor coupled to the first memory and the first network interface, the first computer processor configured to:

~~compute one or more disbursement amounts by applying a disbursement function to:~~

~~at least one of the first principal amount or the second principal amount, and~~

~~a value from at least one of the first data source or the second data source;~~

read the first private key from the first ~~key pair sector~~ memory;

compute a first cryptographic signature from the first private key;

create an inchoate ~~disbursement transaction~~data record comprising:

a commit input for receiving a commit ~~amount~~ data from a commit transaction;

one or more ~~disbursement~~ outputs ~~comprising~~ obtained from ~~the disbursement amounts~~at least one of the first principal data or the second principal data, and a value data from at least one of the first data source or the second data source; and

the first cryptographic signature; and

publish the inchoate ~~disbursement transaction~~data record to at least one of the first client device ~~and~~or the second client device;

the first client device comprising:

a second memory ~~comprising a second key pair sector~~ for storing a second asymmetric key pair, the second asymmetric key pair comprising a second private key and a second public key;

a second network interface; and

a second computer processor coupled to the second memory and the second network interface, the second computer processor configured to:

read the second private key from the second ~~key pair sector~~ memory;

read the inchoate ~~disbursement transaction~~data record;

compute a second cryptographic signature from the second private key;

create a complete ~~disbursement transaction~~ data record comprising:

the commit input;

the ~~disbursement~~ outputs data;

the first cryptographic signature; and

the second cryptographic signature; and

create a ~~disbursement~~ transaction by submitting the complete ~~disbursement transaction~~ data record to the transfer mechanism; ~~and~~

the second client device comprising:

a third memory ~~comprising a third key pair sector~~ for storing a third asymmetric key pair, the third asymmetric key pair comprising a third private key and a third public key;

a third network interface; and

a third computer processor coupled to the third memory and the third network interface, the third computer processor configured to read the third private key from the third ~~key pair sector~~ memory; and

the transfer mechanism comprising the decentralized digital currency that is accessible via a computer network by the computing device, the first client device, and the second client device, respectively, the transfer mechanism configured to broadcast the complete data record to the computer device, the first client device, and the second client device for verifying and effecting the transaction,

wherein an external state is observed by each of the computer device, the first client device, and the second client device, and the transaction is effected when an action by at least two of the computer device, the first client device, or the second client device is detected based on the observed external state.

13. (**Canceled**)

14. (**Canceled**)

15. (**Currently Amended**) The system of claim 12, where the first computer processor is further configured to:

compute a third cryptographic signature from the first private key;

create ~~an~~ another inchoate ~~refund transaction~~data record comprising:

a commit input for receiving the commit ~~amount~~ data from the commit transaction;

a refund output comprising a refund ~~amount~~data; and

the third cryptographic signature; and

publish the another inchoate ~~refund transaction~~data record to at least one of the first client and the second client.

16. (**Currently Amended**) The system of claim 12, where:

the first ~~key pair sector~~memory further stores a fourth asymmetric key pair, the fourth asymmetric key pair comprising a fourth private key and a fourth public key;

the first computer processor is further configured to:

~~compute~~ obtain the one or more ~~disbursement amounts~~ output data ~~by applying the disbursement function to:~~based on:

the first principal ~~amount~~ data; and

the value data from the first data source;

read the fourth private key from the first ~~key pair sector~~ memory;

compute a third cryptographic signature from the fourth private key;

create a commit transaction data record comprising:

a first principal input for receiving the first principal ~~amount~~ data from a first principal transaction;

a commit output comprising the commit ~~amount~~data; and

the third cryptographic signature; and

create the commit transaction by submitting the commit transaction data record to the transfer mechanism.

17. (**Currently Amended**) The system of claim 16, where the second computer processor is configured to:

compute a fourth cryptographic signature from the second private key;

create a first principal transaction data record comprising:

a first principal output comprising the first principal ~~amount~~data; and

the fourth cryptographic signature; and

create the first principal transaction by submitting the first principal transaction data record to the transfer mechanism.

18. (**Canceled**)

19. (**Canceled**)

20. (**Currently Amended**) The system of claim 12, where:

the reference to at least one of the first data source or the second data source comprises at least one of a reference to a base instrument or a reference to a quote instrument; and

the first computer processor is further configured to ~~compute~~ obtain the ~~disbursement amounts~~output data on or after the expiration timestamp.

21. (**Canceled**)

22. (**Canceled**)

23. (**Currently Amended**) The system of claim 12, where:

the second computer processor is further configured to:

compute a third cryptographic signature from the second private key;

create a first principal transaction data record comprising:

a first principal output comprising the first principal ~~amount~~data; and

the third cryptographic signature; and

create a first principal transaction by submitting the first principal transaction data record to the transfer mechanism; and

the third computer processor is further configured to:

compute a fourth cryptographic signature from the third private key;

create a second principal transaction data record comprising:

a second principal output comprising the second principal ~~amount~~data; and

the fourth cryptographic signature; and

create a second principal transaction by submitting the second principal transaction data record to the transfer mechanism.

24. (**Currently Amended**) A method for ~~facilitating value transfers~~ processing a transaction between ~~a first party utilizing~~ a first client device and ~~a second party utilizing~~ a second client device via a transfer mechanism, the transfer mechanism comprising a decentralized digital currency that is accessible via a computer network by a computer device, the first client device, and the second client device, respectively, the method comprising:

storing a first asymmetric key pair in ~~a first key pair sector of~~ a first memory, the first asymmetric key pair comprising a first private key and a first public key;

storing a second asymmetric key pair ~~in a second key pair sector of~~ a second memory, the second asymmetric key pair comprising a second private key and a second public key;

storing a third asymmetric key pair in the second ~~key pair sector~~ memory, the third key pair comprising a third private key and a third public key;

storing a fourth asymmetric key pair in ~~a third key pair sector of~~ a third memory, the fourth asymmetric key pair comprising a fourth private key and a fourth public key;

transmitting terms from one of the first or second client device via a first network interface, the terms comprising:

at least one of a first principal ~~amount~~ data or a second principal ~~amount~~ data;

a reference to at least one of a first data source or a second data source; and

an expiration timestamp;

receiving the terms at ~~a facilitator~~ the computer device via a second network interface;

~~computing one or more disbursement amounts by applying a disbursement function to:~~

~~at least one of the first principal amount or the second principal amount, and~~

~~a value from at least one of the first data source or the second data source;~~

reading the first private key from the first ~~key pair sector~~ memory;

computing a first cryptographic signature from the first private key;

creating a first principal transaction data record comprising:

a first principal output comprising the first principal ~~amount~~data; and

the first cryptographic signature;

creating a first principal transaction by submitting the first principal transaction data record to the transfer mechanism;

reading the second private key from the second ~~key pair sector~~ memory;

computing a second cryptographic signature from the second private key;

creating a commit transaction data record comprising:

a first principal input for receiving the first principal ~~amount~~ data from the first principal transaction;

a commit output comprising a commit ~~amount~~data; and

the second cryptographic signature;

creating the commit transaction by submitting the commit transaction data record to the transfer mechanism;

retrieving a value data from the first data source;

reading the third private key from the second ~~key pair sector~~ memory;

computing a third cryptographic signature from the second private key;

creating an inchoate ~~disbursement transaction~~ data record comprising:

a commit input for receiving a commit ~~amount~~ data from ~~a~~ the commit transaction;

one or more ~~disbursement~~ output~~s~~ data ~~comprising~~ obtained from~~the one or more disbursement amounts~~ the at least one of the first principal data or the second principal data and the value from the first data source; and

the third cryptographic signature;

publishing the inchoate ~~disbursement transaction~~ data record;

reading the inchoate ~~disbursement transaction~~ data record;

reading the fourth private key from the third ~~key pair sector~~ memory;

computing a fourth cryptographic signature from the fourth private key;

creating a complete ~~disbursement transaction~~ data record comprising:

the commit input;

the one or more ~~disbursement outputs~~output data;

the third cryptographic signature; and

the fourth cryptographic signature; ~~and~~

creating a ~~disbursement~~ transaction by submitting the complete ~~disbursement transaction~~ data record to the transfer mechanism;

broadcasting, via the transfer mechanism comprising the decentralized digital currency, the complete transaction record to the computing device, the first client device, and the second client device for verifying and effecting the transaction;

observing an external state; and

effecting the transaction when an action by at least two of the computing device, the first client device, or the second client device is detected based on the observed external state.

25. (**Canceled**)

26. (**Currently Amended**) The method of claim24, further comprising:

computing a fifth cryptographic signature from the third private key;

creating ~~an~~ another inchoate ~~refund transaction~~data record comprising:

a commit input for receiving the commit ~~amount~~ data from the commit transaction;

a refund output comprising a refund ~~amount~~data;

the fifth cryptographic signature; and

a lock time; and

publishing the another inchoate ~~refund transaction~~data record.

27. (**Canceled**)

28. (**Currently Amended**) The method of claim 24, further comprising:

storing a fifth asymmetric key pair in ~~a fourth key pair sector of~~ a fourth memory, the fifth asymmetric key pair comprising a fifth private key and a fifth public key;

reading the fifth private key from the fourth ~~key pair sector~~ memory;

computing a fifth cryptographic signature from the fifth private key;

creating a second principal transaction data record comprising:

a second principal output comprising the second principal ~~amount~~data; and

the fifth cryptographic signature;

creating a second principal transaction by submitting the second principal transaction data record to the transfer mechanism;

computing one or more ~~disbursement amounts~~ output data by applying a disbursement function to:

the value data from the first data source; and at least one of:

the first principal ~~amount~~data; and

the second principal ~~amount~~ data;.

29. (**Currently Amended**) The method of claim 28, further comprising:

computing a sixth cryptographic signature from the third private key;

creating ~~an~~ another inchoate ~~refund transaction~~ data record comprising:

a commit input for receiving the commit ~~amount~~ data from the commit transaction;

one or more refund outputs comprising one or more refund ~~amounts~~data;

the sixth cryptographic signature; and

a lock time; and

publishing the another inchoate ~~refund transaction~~ data record.

30. (**Canceled**)

31. (**Currently Amended**) The method of claim 24, wherein the one or more ~~disbursement~~ output data further comprise one or more conditions requiring approval of at least one of the first ~~party~~ client device or the second ~~party~~ client device, and the one or more conditions include a condition to determine if a sum of the one or more ~~disbursement amounts~~ output data is equal or less than the commit ~~amount~~ data from the commit transaction.

32. (**New**) The method of claim 24, where the first client device and the second client device do not trust each other, and the computer device is not fully trusted by the first client device or the second client device.

STATEMENT OF SUBSTANCE OF INTERVIEW OF SEPTEMBER 15, 2020

(A) Exhibit shown: None.

(B) Identification of the claims discussed: Claim 24

(C) Identification of cited references discussed: See below

(D) Identification of the proposed amendments discussed: Claim 24

(E) Identification of arguments discussed: See below

(F) Other matters discussed: See below

(G) Outcome of the interview: The rejections of Claim 24, and proposed claim amendments were discussed. The Examiner indicated that "redrafting the claim to involve less of a financial nature" would be helpful to overcome the rejections pending further search and consideration. No agreement was reached.

Electronic Acknowledgement Receipt

EFS ID:	41318648
Application Number:	15309612
International Application Number:	
Confirmation Number:	2321
Title of Invention:	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers
First Named Inventor/Applicant Name:	Reginald Middleton
Customer Number:	86636
Filer:	Misung Lee/Juel Clyne
Filer Authorized By:	Misung Lee
Attorney Docket Number:	4675.1002BS
Receipt Date:	08-DEC-2020
Filing Date:	08-NOV-2016
Time Stamp:	11:42:43
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	$740
RAM confirmation Number	E2020B8B43017773
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	Amendment/Req. Reconsideration-After Non-Final Reject	4675_20201208_NFOA_Response.pdf	313125 2eaeee68e35da929242b078d8307a0b8aa44c8bf	no	46
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30832 29c0608caf3b0c01b1439d4890adb228da071b76	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	343957		

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.

REMARKS

The courtesy and cooperation shown by the Examiner during the telephone interview of September 15, 2020, are appreciated. During the interview, multiple proposals/amendments to address the rejections under 35 U.S.C. §§ 101 and 103 were discussed. Further, no formal agreement is believed to have been reached regarding the allowability of the claims. The claims have been amended herein based on the discussion during the interview. Reconsideration and allowance in view of the foregoing amendments and the following remarks are respectfully requested.

Claims 1, 3-6, 9, 12, 15-17, 20, 23, 24, 26, 28, 29 and 31 were pending. **Claims 1, 3-6, 9, 12, 15-17, 20, 23, 24, 26, 28, 29 and 31** were rejected under 35 U.S.C. § 101. **Claims 1, 3-6 and 9** were rejected under § 35 U.S.C. § 112(b). **Claims 2 and 12-30** were rejected under 35 U.S.C. § 103. Upon entry of the amendment, **Claims 1, 3-6,9, 12, 24 and 28** are currently amended. Support for the amendments to independent **Claims 1, 12, and 24** can be found, at least at, paragraphs **[0031]-[0034], [0052], [0053], [0337], [0339], and [0340], and FIG. 1** of the U.S. Patent Application Publication. Support for new **Claim 32** can be found, at least at, paragraph [0063] of the U.S. Patent Application Publication. No new matter is added.

Favorable consideration is respectfully requested.

CLAIM REJECTION UNDER 35 U.S.C. § 101

Claims 1, 3-6, 9, 12, 15-17, 20, 23, 24, 26, 28, 29 and 31 *are rejected under 35 U.S.C. § 101 as allegedly being directed to an abstract idea without significantly more.*

Applicant traverses the rejection, and respectfully requests that the rejection be reconsidered and withdrawn. Among independent **Claims 1, 12, and 24**, Applicant will discuss **Claim 24** as being representative, but only to the extent that similar features are recited in all three independent claims. Applicant submits that the scope and features of the independent claims are not identical.

The "2019 Revised Patent Subject Matter Eligibility Guidance" (hereafter "Revised Guidance"), effective by the USPTO as of January 7, 2019, has been issued and revised procedures for determining whether a patent claim or patent application claim is directed to a judicial exception and has explained that a patent claim or patent application claim that recites a judicial exception is not directed to the judicial exception if the judicial exception is integrated into a practical application of the judicial exception. Further, the "October 2019 Patent Eligibility Guidance Update" (hereafter "Update"), effective by the USPTO as of October 17, 2019, has been issued.

The Revised Guidance and the Update instruct the Examining Corps to first determine whether claims are directed to one of four statutory categories of invention. If the claim does fall within one of the statutory categories, the Examining Corps is instructed use the analysis, as explained below.

STEP 1 – DETERMINE WHETHER THE CLAIMS ARE DIRECTED TO ONE OF FOUR STATUTORY CATEGORIES OF INVENTION

In Step 1, a determination is made as to whether the claim is directed to a process, machine, manufacture, or composition of matter. In the present application, there is no dispute that Step 1 has been met as **Claim 24** is directed to a method which is one of four statutory categories of invention. As **Claim 24** is directed to a statutory category, analysis under Step 2 follows, as described below.

STEP 2A – PRONG 1: "WHETHER THE CLAIM RECITES A JUDICIAL EXCEPTION"

Prong 1 of Step 2A of the analysis in Revised Guidance instructs USPTO Examiners should evaluate "whether the claim recites a judicial exception, i.e., an abstract idea, a law of nature, or a natural phenomenon," and "[t]o determine whether a claim recites an abstract idea in Prong One, examiners are now to: (a) Identify the specific limitation(s) in the claim under examination (individually or in combination) that the examiner believes recites an abstract idea; and (b) determine whether the identified limitation(s) falls within the subject matter groupings of abstract ideas." Further, Prong 1 of Step 2A of the analysis states, the abstract idea exception includes the following groupings of subject

matter, when recited as such in a claim limitation(s) (that is, when recited on their own or per se):

> (a) Mathematical concepts— mathematical relationships, mathematical formulas or equations, mathematical calculations;
>
> (b) Certain methods of organizing human activity—fundamental economic principles or practices (including hedging, insurance, mitigating risk); commercial or legal interactions (including agreements in the form of contracts; legal obligations; advertising, marketing or sales activities or behaviors; business relations); managing personal behavior or relationships or interactions between people (including social activities, teaching, and following rules or instructions); and
>
> (c) Mental processes—concepts performed in the human mind (including an observation, evaluation, judgment, opinion).

Turning to the Office Action, at pages 26-27, it is alleged that:

> The claim falls within two groupings of abstract ideas involving the ***organizing of human activity*** as indicated in the 2019 Revised Patent Subject Matter Eligibility Guidance, one of which is the processing of a payment between two parties which falls under the category of a ***fundamental economic practice***. As the claim also recites that the transaction requires particular signatures of the intermediary and the first client the claim can also be viewed as falling within the category of ***a commercial/legal interaction*** involving a contract involving terms including principal amounts, references to data sources and expiration of the terms i.e. requiring that the contract be consummated within a specified period of time that result in the creation of a disbursement transaction record including amounts, values, signatures and commitment inputs that are then published to both parties to the contract. The disclosure itself recites at paragraph 108 that "The invention pertains to agreements among distinct parties that contemplate transfer of title to property, as well as any industry where that may be of value or importance" and clearly falls within the grouping of commercial/legal interactions under the groupings. Therefore under the analysis made under prong one of step 2A the claim is determined to be ineligible.

Applicant respectfully disagrees. Nevertheless, without conceding the propriety of the rejection, but rather as a cooperative effort to expedite the prosecution of this application to allowance, Applicant has amended **Claim 24** to address the rejection.

Currently amended **Claim 24** recites (emphasis added):

A method for ***processing a transaction between a first client device and a second client device via a transfer mechanism, the transfer mechanism comprising a decentralized digital currency that is accessible via a computer network by a computer device, the first client device, and the second client device, respectively***, the method comprising:

storing a first asymmetric key pair in a first memory, the first asymmetric key pair comprising a first private key and a first public key;

storing a second asymmetric key pair a second memory, the second asymmetric key pair comprising a second private key and a second public key;

storing a third asymmetric key pair in the second memory, the third key pair comprising a third private key and a third public key;

storing a fourth asymmetric key pair in a third memory, the fourth asymmetric key pair comprising a fourth private key and a fourth public key;

transmitting terms from one of the first or second client device via a first network interface, the terms comprising:

at least one of a first principal data or a second principal data;

a reference to at least one of a first data source or a second data source; and

an expiration timestamp;

receiving the terms at the computer device via a second network interface;

reading the first private key from the first memory;

computing a first cryptographic signature from the first private key;

creating a first principal transaction data record comprising:

a first principal output comprising the first principal data; and

the first cryptographic signature;

creating a first principal transaction by submitting the first principal transaction data record to the transfer mechanism;

reading the second private key from the second memory;

computing a second cryptographic signature from the second private key;

creating a commit transaction data record comprising:

a first principal input for receiving the first principal data from the first principal transaction;

a commit output comprising a commit data; and

the second cryptographic signature;

creating the commit transaction by submitting the commit transaction data record to the transfer mechanism;

retrieving a value data from the first data source;

reading the third private key from the second memory;

computing a third cryptographic signature from the second private key;

creating an inchoate data record comprising:

a commit input for receiving a commit data from the commit transaction;

one or more output data obtained from the at least one of the first principal data or the second principal data and the value from the first data source; and

the third cryptographic signature;

publishing the inchoate data record;

reading the inchoate data record;

reading the fourth private key from the third memory;

computing a fourth cryptographic signature from the fourth private key;

creating a complete data record comprising:

the commit input;

the one or more output data;

the third cryptographic signature; and

the fourth cryptographic signature;

creating a transaction by submitting the complete data record to the transfer mechanism;

broadcasting, via the transfer mechanism comprising the decentralized digital currency, the complete transaction record to the computing device, the first client device, and the second client device for verifying and effecting the transaction;

observing an external state; and

effecting the transaction when an action by at least two of the computing device, the first client device, or the second client device is detected based on the observed external state.

In contrast to the above allegations by the Office Action, currently amended **Claim 24** is directed to a specific method for enabling increased security for either party entering into the transaction via the decentralized digital currency of the transfer mechanism, without requiring expensive tamper-proof electronic units. Furthermore, the computing device as recited in **Claim 24** participates in the transaction but the computing device alone does not control disposition. Instead, the computing device only effects the transaction between the client devices in conjunction with the participation of one of the first or second client device and either the first or second client device is responsible for ultimately administering the transaction via the *decentralized digital currency.* The claimed decentralized digital currency prevents the computer device from being commandeered to effect transaction not contemplated by at least one of the first or second client device. As such, by definition, the computer

device is a *distributed participant* that works in connection with the first and second client device, but that does not make it centralized, thereby enabling transaction *without involving costly third-party intermediaries who traditionally may otherwise be required, and without traditional exposure to counterparty risk*. Therefore, amended **Claim 24** is not simply "fundamental economic practice" or "a commercial/legal interaction," as alleged by the Office Action. It is respectfully submitted that the feature of amended **Claim 24** is implemented on the *decentralized digital currency* that is not to be a "fundamental" economic practice or "a commercial/legal interaction."

At least in view of the current amendments, Applicant respectfully submits that currently amended **Claim 24** does not fall into "organizing of human activity" or any of three groupings of abstract ideas, and that Prong 1 of Step 2A must be answered "NO."

STEP 2A – PRONG 2: "WHETHER THE JUDICIAL EXCEPTION IS INTEGRATED INTO A PRACTICAL APPLICATION"

Prong 2 of Step 2 of the analysis in Revised Guidance instructs that:

> [E]xaminers should evaluate ***whether the claim as a whole integrates the recited judicial exception into a practical application of the exception***. A claim that integrates a judicial exception into a practical application will apply, rely on, or use the judicial exception ***in a manner that imposes a meaningful limit on the judicial exception, such that the claim is more than a drafting effort designed to monopolize the judicial exception***. When the exception is so integrated, then the claim is not directed to a judicial exception (Step 2A: NO) and is eligible.

Further, Prong 2 of Step 2 of the analysis states that:

> Examiners evaluate integration into a practical application by: (a) Identifying whether there are any additional elements recited in the claim beyond the judicial exception(s); and (b) ***evaluating those additional elements individually and in combination to determine whether they integrate the exception into a practical application, using one or more of the considerations***...

Examples in the Revised Guidance that are indicative that an additional element (or combination of elements) may have "integrated the exception into a practical application" include (*emphasis added*):

- An additional element reflects ***an improvement in the functioning of a computer, or an improvement to other technology or technical field***;
- An additional element that applies or uses a judicial exception to effect a particular treatment or prophylaxis for a disease or medical condition;
- An additional element implements a judicial exception with, or uses a judicial exception in conjunction with, a particular machine or manufacture that is integral to the claim;
- An additional element effects a transformation or reduction of a particular article to a different state or thing; and
- An additional element applies or uses the judicial exception in ***some other meaningful way beyond generally linking the use of the judicial exception to a particular technological environment, such that the claim as a whole is more than a drafting effort designed to monopolize the exception.***

The Office Action, at pages 27-28, further alleges:

> The structural elements in the claim are limited to what is described as a "transfer mechanism", three memories and two network interfaces along with recitations of first and second clients in the preamble. The claim also recites the capability of encryption by taking a private key and computing a cryptographic signature. In reviewing the written disclosure at paragraphs 52-53, 106 and 113 the memory and network interface are described in a manner that includes no technological improvement to the functioning of the memory and network interface and only describes a particular technological environment for which an intermediary described in paragraph 113 as a "facilitator" is linked. With regard to the encryption capabilities no particular algorithm for computing a signature is described in the written disclosure beyond the recitations at pages 17, 18 and 28 that in order to consummate a transaction that a plurality of signatures are required and ***the function is described at a generally high level by the written disclosure such that in the broadest reasonable interpretation the claim scope encompasses encryption that could be performed by human beings.*** Even if a computer calculation of the signature were inferred from the claim the written disclosure relies on prior art signature calculation mechanisms such as multisignature transactions (see footnote 2 of page 4 of the written disclosure) or P2SH (97 and 104 of the written disclosure) and therefore do not constitute any technological improvement to the functioning of the computer itself. With regard to the two clients paragraph 110 in describing the client also describes a generic computing device with no technological improvement.

Applicant respectfully disagrees.

In In 2019 PEG Example 40 ("Example 40"), issued January 7, 2019, although each of the collecting steps analyzed individually may be viewed as mere pre- or post-solution activity, the claim as a whole is directed to a particular improvement in collecting traffic data. Specifically, the method ***limits collection of additional Netflow protocol data to when the initially collected data reflects an abnormal condition***, which avoids excess traffic volume on the network and hindrance of network performance, and the collected data can then be used to analyze the cause of the abnormal condition. Therefore, in Example 40, ***a specific improvement over prior systems, resulting in improved network monitoring, is provided***, and therefore, the claim as a whole integrates the mental process into a practical application.

Similar to Example 40, amended **Claim 24** recites the method that ***limits effecting of the complete disbursement transaction to when an action by at least two of the network participants is detected based on the observed external state***. Therefore, the claimed method enables network participants to interact effectively and automatically each other based on an observed change of the state, and thus, ***avoids involvement of expensive third party intermediaries***. At the same time, increased security for either party entering into the transaction via the decentralized digital currency is enabled and the counter party risk can be mitigated from a value transfer among multiple parties. Accordingly, like Example 40, amended **Claim 24,** as a whole, integrates the judicial exception into a practical application.

In 2019 PEG Example 41 ("Example 41"), issued January 7, 2019, the combination of additional elements use the mathematical formulas and calculations in ***a specific manner that sufficiently limits the use of the mathematical concepts to the practical application of transmitting the ciphertext word signal to a computer terminal over a communication channel***, and the mathematical concepts are ***integrated into a process that secures private network communications***. Therefore, in Example 41, a ciphertext word signal can be transmitted between computers of people who do not know each other or who have not shared a private key between them in advance of the message being transmitted, where

the security of the cipher relies on the difficulty of factoring large integers by computers, and thus the claim is not directed to the recited judicial exception.

Similar to Example 41, amended **Claim 24** is directed to a specific method for enabling increased security for either party entering into the transaction via the decentralized digital currency of the transfer mechanism, *without requiring expensive tamper-proof electronic units and without involving costly third-party intermediaries who traditionally may otherwise be required, and traditional exposure to counterparty risk.* At least the above emphasized features of amended **Claim 24** solve a problem of conventional transaction that requires expensive tamper-proof electronic units for enhanced security and also requires involvement of expensive third party intermediaries. In contrast to the allegation of "***the function [being] described at a generally high level by the written disclosure such that in the broadest reasonable interpretation the claim scope encompasses encryption that could be performed by human beings***," as alleged by the Office Action, Applicant submits that amended **Claim 24** is directed to an improvements in processing transaction technology, particularly, via a transfer mechanism comprising a decentralized digital currency with enhanced security. At least the above emphasized features of amended **Claim 24**, for example, permits providing enhanced security for either party entering into the transaction via the decentralized digital currency of the transfer mechanism, without requiring expensive tamper-proof electronic units, because the decentralized digital currency of the transfer mechanism requires that transactions are validated by a number of participants in the network before the transaction actually occurs and is recorded on the ledger. In this regard, a part or whole of paragraphs [0010] and [0011] of the U.S. Patent Application Publication as reproduced below:

> [0010] For the purposes of illustration by way of non-limiting example, ***those particular decentralized digital currencies generally operate by maintaining a whole or partial history or "ledger" (sometimes referred to as a "block chain") of all transactions that have been "validated" by a consensus of network participants.*** With few exceptions beyond the scope of the invention, transactions function roughly as follows.<2 >A transaction comprises at least one input and at least one output. The

> input comprises an input "script", which comprises an ordered set of well-defined executable operations. The output comprises an output script, which comprises a second ordered set of such operations. A new (child) transaction comprises an input whose input script is combined with the output script from an existing (parent) transaction in a predictable way. ***The new transaction is considered valid if a majority of network participants agree that the combination, when evaluated according to a predetermined set of rules, produces an anticipated state or result…***
>
> [0011] More specifically, the entity seeking to submit a new transaction to the ledger transmits (or "broadcasts") a transaction record comprising the details of the desired transaction to a number of network participants then known to the entity (or "peers"). Those peers typically attempt to independently validate the transaction record. If successful, they rebroadcast the transaction record to their peers, and so on. ***Eventually the transaction record is received by a network participant who is configured to effect the transaction by including the transaction record in the ledger (i.e., in a valid "block");*** see more detailed description below).

In particular, the claimed "***creating a first principal transaction by submitting the first principal transaction data record to the transfer mechanism***;" "***creating the commit transaction by submitting the commit transaction data record to the transfer mechanism***"; "***creating a transaction by submitting the complete data record to the transfer mechanism***;" "***broadcasting, via the transfer mechanism comprising the decentralized digital currency, the complete transaction record to the computing device, the first client device, and the second client device for verifying and effecting the transaction***; ***observing an external state; and effecting the transaction when an action by at least two of the computing device, the first client device, or the second client device is detected based on the observed external state***," enables the transaction data record being made available for verification to all participants of the decentralized digital currency network, who can independently verify the transaction data record before the transaction is actually effected when one participant adds the transaction to the ledger. Therefore, involvement of expensive third-party intermediaries can be avoided and counter party risk can be mitigated from enabling transactions among multiple parties.

Accordingly, Applicant respectfully submits that amended **Claim 24** is directed to an

improvement in technology, similar to eligible claims in *McRO or DDR*, and is integrated into a practical application of the judicial exception, as required by the Revised Guidance.

Furthermore, in contrast to the allegation that the function is described at a generally high level that could be performed by human beings as alleged by the Office Action, amended **Claim 24** recites "the transfer mechanism comprising a decentralized digital currency." It is respectfully submitted that, by definition, participation with a ***decentralized*** digital currency is done so with a device and in a manner in which human beings have never acted previously. A decentralized currency that exists solely outside of that context (e.g., one that is devoid of a network of participants) would be worthless, which is why the claims are limited to decentralized digital currencies, not other types of currencies. Further, decentralized digital currencies are worthless without decentralized participants and a distributed physical data record of transactions that record cryptographic solutions as a means of proving authority to effect transfers. Prior to the present application, no human had demonstrated application of this technology to accomplish the goals of the present application at all, much less in the manner in which the present application presents. Further, before the present application, it was physically impossible for an intermediary (human or otherwise) to control disposition without additional participants.

The Office Action further alleges, at pages 28-29, that:

> ***The transfer mechanism per paragraphs 53, 54 and 96 are not elements of physical structure but instead are protocols involving at least decentralized currency ("Where a decentralized digital currency [e.g., the Bitcoin protocol, the Ethereum protocol, or similar] is used as the transfer mechanism…", 96) but per paragraph 49 can also involve centralized currency and the broadest reasonable interpretation of the term transfer mechanism can be viewed as any form of monetary exchange scheme. If the combination of transfer mechanism, memory, network interfaces and two clients are considered there is no meaningful technological contribution being made in the form of a combination of elements as the transfer mechanism and clients merely represent the computer equivalents of two parties to a contract in which an intermediary is used through the network interfaces and therefore the combination as a whole is merely a mechanism for linking the abstract idea to a particular technological environment.*** Therefore under prong two of Step 2A no practical application of the

> abstract idea is present in the claim and the result of the analysis is that the claim is still ineligible.

Applicant respectfully disagrees and points out that nowhere does the present application suggests that conventional centralized transfer mechanisms can achieve improvements of the technologies enabled by amended **Claim 24** as implemented on the decentralized digital currencies.

Amended **Claim 24** is directed to a specific method for the value transfer implemented on the *decentralized digital currency* but not on the centralized currency. The computer device as recited in **Claim 24** participates in the transaction but the computer device alone does not control disposition. Instead, the computer device only effects a transaction in conjunction with the participation of one of the first or second clients and either the first or second client is responsible for ultimately administering the transaction via the *decentralized digital currency.* The claimed decentralized digital currency prevents the computer device from being commandeered to effect the transaction not contemplated by at least one of the first or second client device. As such, by definition, the computer device is a distributed participant that works in connection with the first and second client devices, but that does not make it centralized. For example, paragraphs [0009], [0015], [0016], and [0018] of the U.S. Patent Application Publication state, in part or whole (emphasis added):

> [0009] Decentralized digital currencies (or so-called "cryptocurrencies")—technologies that promise ***tightly-controlled asset creation*** coupled with the ability to ***transfer control or ownership of those assets computationally when rigorously-defined criteria are met***, ***with little-or-no dependency on third party intermediaries***, and with very low transaction costs compared to traditional mechanisms—are relatively new creatures. ***The Bitcoin protocol*** and progeny (Ethereum, Litecoin, etc.) are ***one such class of technologies*** that have recently enjoyed meteoric rises in popularity (and valuation).
>
> [0015] … While this section often refers to "***Bitcoin***" by name, the description is accurate for nearly ***all of the decentralized digital currencies*** currently known in the art…
>
> [0016]… A novel solution accomplishes this ***without any trusted central authority: maintenance of the block chain is performed by a network***

> ***of communicating nodes running bitcoin software***…
>
> [0018] … Ownership of bitcoins implies that a user can spend bitcoins associated with a specific address. To do so, a payer must digitally sign the transaction using the corresponding private key. Without knowledge of the private key the transaction cannot be signed and bitcoins cannot be spent. The network verifies the signature using the public key. If the private key is lost, the bitcoin network will not recognize any other evidence of ownership; the coins are then unusable, and thus effectively lost. For example, in 2013 one user said he lost 7,500 bitcoins, worth $7.5 million at the time, when he discarded a hard drive containing his private key…

Furthermore, paragraph [0025] of the U.S. Patent Application Publication states:

> [0025] The invention pertains to ***systems and methods enabling parties with little trust or no trust in each other to enter into and enforce agreements conditioned on input from or participation of a third party, over arbitrary distances, without special technical knowledge of the underlying transfer mechanism(s), optionally affording participation of third-party mediators, substitution of transferors and transferees, term substitution, revision, or reformation, etc. Such exchanges can occur reliably without involving costly third-party intermediaries who traditionally may otherwise be required, and without traditional exposure to counterparty risk***.

The above recited critical features of *decentralized digital currencies* afford the novelty of a participating facilitator without also allowing that the computer device to control dispositions. Nowhere does the present application suggests that conventional transfer mechanisms can stand in for decentralized digital currencies.

Also, paragraph [0029] of the U.S. Patent Application Publication states:

> [0029] Combinations are possible. For example, Party A accepts Australian dollars (AUD), but prefers USD, and wants to hedge against volatility of AUD in USD. One embodiment of the invention allows Party A to swap exposure to USD in BTC with Party B, and simultaneously swap exposure to BTC in AUD with Party C over a similar time period, thereby synthesizing a hedge against AUD in USD. The invention is not limited such that Party B and Party C are distinct parties (they could be the same), nor is it limited such that such that Party A must conduct two separate trades. In addition, various embodiments of the invention allow the parties to perform these types of transactions without maintaining currency deposits or making currency purchases or

exchanges.

As set forth above, paragraph [0029] of the U.S. Patent Application Publication describes how to synthesize a swap transaction using the features as described in the present application. It does not contemplate removing the characteristics of decentralized digital currencies that afford the aforementioned features. Implementing the benefits of the present application would not be possible using conventional transfer mechanisms, which all involve third party intermediaries who temporarily control disposition of transfers. That is, the present application implemented on the decentralized digital currencies affords transactions between parties where no intermediary has an opportunity to behave badly or incompetently, thereby mitigating counterparty risk.

Accordingly, Applicant respectfully submits that amended **Claim 24** is directed to an improvement in technology and is integrated into a practical application of the judicial exception, as required by the Revised Guidance.

At least in view of the current amendments, Applicant respectfully submits that amended **Claim 24** does not fall into any of the three groupings of abstract ideas, and even if **Claim 24** recites an abstract idea, **Claim 24** integrates the recited judicial exception into a practical application of the exception, and that Prong 2 of Step 2A must be answered "YES."

STEP 2B - PART 2 OF THE "TWO-PART ANALYSIS FOR ABSTRACT IDEAS"

Even if a claim has been determined to be directed to a judicial exception under revised Step 2A, Step 2B of the analysis in Revised Guidance instructs "examiners should then evaluate the additional elements individually and in combination under Step 2B to determine whether they provide an inventive concept (i.e., whether the additional elements amount to significantly more than the exception itself)."

Still, even if evidence were to be offered, Applicant submits that amended **Claim 24** recites significantly more than the alleged abstract idea.

In the rejection of previously-presented **Claim 24**, the Office Action, at pages 29-32, alleges:

> Even if a computer calculation of the signature were inferred from the claim the written disclosure relies on prior art signature calculation mechanisms such as multisignature transactions (see footnote 2 of page 4 of the written disclosure) or P2SH (97 and 104 of the written disclosure) and therefore ***do not constitute any technological improvement to the functioning of the computer itself.*** With regard to the two clients paragraph 110 in describing the client also describes ***a generic computing device with no technological improvement***. ***The transfer mechanism per paragraphs 53, 54 and 96 are not elements of physical structure but instead are protocols involving at least decentralized currency ("Where a decentralized digital currency [e.g., the Bitcoin protocol, the Ethereum protocol, or similar] is used as the transfer mechanism…", 96) but per paragraph 49 can also involve centralized currency and the broadest reasonable interpretation of the term transfer mechanism can be viewed as any form of monetary exchange scheme. No technological improvement is recited in the claim nor does the combination of memories, network interfaces, transfer mechanism and two clients serve to form an ordered combination of elements that results in any technological improvement.*** It is abundantly clear that the claim does not involve any ordered combination of elements as the recited transfer mechanism along with the two clients ***do not utilize any special properties of a network or distributed computing in order to gain any technological improvement and merely are directed towards a centralized, "one-size-fits-all" technological implementation and the clients merely serve as representatives of human counterparts engaging in a contract*** …
>
> However in the instant claims the recited operations of transferring payments and utilizing trusted intermediaries in making a payment as part of a contractual relationship are all operations that have previously been done by human beings in the same manner being claimed. … as there is nothing in the claims themselves or even in the written description to explicitly state or even implicitly suggest that the claims involve anything more than generic computer operations. …nothing within the claim or the four corners of the written description provides any teaching or suggestion of an improved computer algorithm for analyzing data such as the self-referential table of Enfish that brings about an improvement to the computer itself where Enfish taught that the claimed invention brought about "increased flexibility, faster search times, and smaller memory requirements" (Enfish at 1690). There is also no technological improvement being made to any external technology (Diamond v. Diehr, 450 U.S. 175, 184 (1981)). The written disclosure at paragraphs 52-53, 106, 110 and 113 describe only the use of ***a generic unimproved computing environment and describes the elements in a manner that indicates that the additional elements are sufficiently well-known*** that the specification does not need to describe the particulars of such additional elements to satisfy 35 U.S.C. §112 (a)

> and the disclosure itself recites at paragraph 108 that "The invention pertains to agreements among distinct parties that contemplate transfer of title to property, as well as any industry where that may be of value or importance" and clearly falls within the grouping of commercial/legal interactions under the groupings.

Applicant disagrees and submits that amended **Claim 24** recites significantly more than the alleged abstract idea.

As discussed above, it is respectfully submitted that the claimed combination improves a transaction technology, via a transfer mechanism comprising a decentralized digital currency with enhanced security and mitigated third party risks. At least the above emphasized features of amended **Claim 24**, for example, permits providing enhanced security for either party entering into the transaction via the decentralized digital currency of the transfer mechanism, without requiring expensive tamper-proof electronic units, because the decentralized digital currency of the transfer mechanism requires that transactions are validated by a number of individual devices before the transaction actually occurs and is recorded on the ledger. Furthermore, implementing specific improvements achieved by the present application would not be possible using conventional transfer mechanisms which all involve third party intermediaries who temporarily control disposition of transfers. That is, the present application implemented on the decentralized digital currencies affords transactions between parties where no intermediary has an opportunity to behave badly or incompetently.

Therefore, currently amended **Claim 24** recites specific improvements over prior methods, resulting in an enhanced value transfer technology implemented on a decentralized digital currency, and does not direct to "a generic computing device with no technological improvement," as alleged by the Office Action.

For at least the foregoing reasons, amended **Claim 24** recites "significantly more" than the alleged abstract idea. Independent **Claims 1 and 12** are similarly amended to recite such feature.

Accordingly, Step 2B is answered "Yes" and all claims are patent eligible. Reconsideration and withdrawal of the rejection are thus respectfully requested. Applicant respectfully requests that the rejection of **Claims 1, 3-6, 9, 12, 15-17, 20, 23, 24, 26, 28, 29, 31 and 32** under 35 U.S.C. § 101 be reconsidered and withdrawn.

CLAIM REJECTION UNDER 35 U.S.C. § 112

Claims 1, 3-6 and 9 *are rejected under 35 U.S.C. § 112(b) or 35 U.S.C. § 112 (pre-AIA), second paragraph, as allegedly 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.*

Without conceding the propriety of the rejections, but rather as a part of cooperative efforts to expedite the prosecution of this application to allowance, Applicant is currently amending **Claims 1, and 3-6**. Accordingly, at least in view of the current amendments, Applicant, therefore, respectfully requests the reconsideration and withdrawal of rejection under 35 U.S.C. § 112(b).

CLAIM REJECTIONS UNDER § 103

Claims 1, 3-6, 9, 12, 15-17, 20, 23, 24, 26, 28, 29 and 31 *rejected under 35 U.S.C. § 103 as allegedly being unpatentable over Rosen (U.S. Publication No. 2003/0070080; hereafter "Rosen") and further in view of Feigelson (U.S. Publication No. 2013/0166455; hereafter "Feigelson").*

Applicant traverses the rejection, and respectfully requests that the rejection be reconsidered and withdrawn.

As set forth above, **Claim 24** is currently amended to recite (emphasis added):

> A method for ***processing a transaction between a first client device and a second client device via a transfer mechanism, the transfer mechanism comprising a decentralized digital currency that is accessible via a computer network by a computer device, the first client device, and the second client device, respectively***, the method comprising:
>
> storing a first asymmetric key pair in a first memory, the first asymmetric key pair comprising a first private key and a first public key;

storing a second asymmetric key pair a second memory, the second asymmetric key pair comprising a second private key and a second public key;

storing a third asymmetric key pair in the second memory, the third key pair comprising a third private key and a third public key;

storing a fourth asymmetric key pair in a third memory, the fourth asymmetric key pair comprising a fourth private key and a fourth public key;

transmitting terms from one of the first or second client device via a first network interface, the terms comprising:

at least one of a first principal data or a second principal data;

a reference to at least one of a first data source or a second data source; and

an expiration timestamp;

receiving the terms at the computer device via a second network interface;

reading the first private key from the first memory;

computing a first cryptographic signature from the first private key;

creating a first principal transaction data record comprising:

a first principal output comprising the first principal data; and

the first cryptographic signature;

creating a first principal transaction by submitting the first principal transaction data record to the transfer mechanism;

reading the second private key from the second memory;

computing a second cryptographic signature from the second private key;

creating a commit transaction data record comprising:

a first principal input for receiving the first principal data from the first principal transaction;

a commit output comprising a commit data; and

the second cryptographic signature;

creating the commit transaction by submitting the commit transaction data record to the transfer mechanism;

retrieving a value data from the first data source;

reading the third private key from the second memory;

computing a third cryptographic signature from the second private key;

creating an inchoate data record comprising:

a commit input for receiving a commit data from the commit transaction;

one or more output data obtained from the at least one of the first principal data or the second principal data and the value from the first data source; and

the third cryptographic signature;

publishing the inchoate data record;

reading the inchoate data record;
reading the fourth private key from the third memory;
computing a fourth cryptographic signature from the fourth private key;
creating a complete data record comprising:
the commit input;
the one or more output data;
the third cryptographic signature; and
the fourth cryptographic signature;
creating a transaction by submitting the complete data record to the transfer mechanism;
broadcasting, via the transfer mechanism comprising the decentralized digital currency, the complete transaction record to the computing device, the first client device, and the second client device for verifying and effecting the transaction;
observing an external state; and
effecting the transaction when an action by at least two of the computing device, the first client device, or the second client device is detected based on the observed external state.

In the rejection of previously presented **Claim 24**, the Office Action, at page 47, acknowledges that Rosen does not explicitly disclose wherein the transfer mechanism comprises a decentralized currency. Then, the Office Action alleges that Feigelson teaches "wherein the transfer mechanism comprises a decentralized currency and it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the electronic monetary system of Rosen with the creation and use of digital currency of Feigelson for the purpose of maintaining secrecy of information in order to control its value." Further, the Response to the Arguments section in the Office Action, at pages 3-4, alleges (emphasis added):

> Applicant's argument with regard to the 35 U.S.C. § 103 (a) rejection of claim 24 has been fully considered but is not persuasive. ***The claim is not claiming the actual mechanisms for implementing a decentralized currency such as the distributed ledger or blockchain but only the intermediary serving to bring agreement and administer the contract between a first party and a second party that involves exchange of value inclusive of a decentralized currency. As such the facilitator clearly is playing a centralized role even if the currency is a decentralized currency and nothing within the claim itself or even the written disclosure of the examined application suggests that the role of the facilitator would in any way be altered based on whether the***

> ***currency was centralized or decentralized. Paragraph 29 of the filed application teaches that combinations between centralized and decentralized currencies are possible and nothing within the claim itself or the written disclosure would suggest that the limiting of the operations to only involve decentralized currency would constitute anything more than a field of use which would not distinguish the claim from the prior art.*** Furthermore given the breadth of the teachings of the Rosen disclosure nothing is present that would suggest that the functions of administrating contracts and payments would be altered based on the nature of the underlying currency. As such those skilled in the art would view Rosen when combined with Feigelson as simply adding a feature not present in Rosen that would entail nothing more than bringing about a predictable result. No specialized teaching is required to add the capability of cryptocurrency to Rosen. As noted in MPEP § 2144 (II) "…the desire to enhance commercial opportunities by improving a product or process is universal—and even common-sensical" and those skilled in the art upon seeing an additional commercial opportunity to enhance Rosen would certainly have relied on Rosen or a similar reference in order to provide the additional capability of interfacing with a cryptocurrency.

Applicant respectfully disagrees.

In contrast to the above allegations that the computer device as claimed "clearly is playing a centralized role," as alleged by the Office Action, Applicant points out that the computer device as recited in **Claim 24** participates in the transaction but the computer device alone does not control disposition. Instead, the computer device only effects the transaction *in conjunction with* the participation of one of the first or second client device and either the first or second client device is responsible for ultimately administering the transaction via the *decentralized digital currency.* The claimed decentralized digital currency prevents the computer device from being commandeered to effect the transaction not contemplated by at least one of the first or second client device. As such, by definition, the computer device is a distributed participant that works in connection with the first and second client device, but that does not make it centralized. For example, paragraphs [0009], [0015], [0016], and [0018] of the U.S. Patent Application Publication state, in part or whole (emphasis added):

> [0009] Decentralized digital currencies (or so-called "cryptocurrencies")—technologies that promise ***tightly-controlled asset***

> ***creation*** coupled with the ability to ***transfer control or ownership of those assets computationally when rigorously-defined criteria are met***, ***with little-or-no dependency on third party intermediaries***, and with very low transaction costs compared to traditional mechanisms—are relatively new creatures. ***The Bitcoin protocol*** and progeny (Ethereum, Litecoin, etc.) are ***one such class of technologies*** that have recently enjoyed meteoric rises in popularity (and valuation).
>
> [0015] … While this section often refers to "***Bitcoin***" by name, the description is accurate for nearly ***all of the decentralized digital currencies*** currently known in the art…
>
> [0016]… A novel solution accomplishes this ***without any trusted central authority: maintenance of the block chain is performed by a network of communicating nodes running bitcoin software***…
>
> [0018] … Ownership of bitcoins implies that a user can spend bitcoins associated with a specific address. To do so, a payer must digitally sign the transaction using the corresponding private key. Without knowledge of the private key the transaction cannot be signed and bitcoins cannot be spent. The network verifies the signature using the public key. If the private key is lost, the bitcoin network will not recognize any other evidence of ownership; the coins are then unusable, and thus effectively lost. For example, in 2013 one user said he lost 7,500 bitcoins, worth $7.5 million at the time, when he discarded a hard drive containing his private key…

As set forth above, critical features of claimed *decentralized digital currencies* afford the novelty of a participating computer device without also allowing that the computer device to control dispositions. Nowhere does the present application suggests that conventional transfer mechanisms can stand in for decentralized digital currencies.

Also, paragraph [0029] of the U.S. Patent Application Publication states:

> [0029] Combinations are possible. For example, Party A accepts Australian dollars (AUD), but prefers USD, and wants to hedge against volatility of AUD in USD. One embodiment of the invention allows Party A to swap exposure to USD in BTC with Party B, and simultaneously swap exposure to BTC in AUD with Party C over a similar time period, thereby synthesizing a hedge against AUD in USD. The invention is not limited such that Party B and Party C are distinct parties (they could be the same), nor is it limited such that such that Party A must conduct two separate trades. In addition, various embodiments of the invention allow the parties to perform these types of transactions without maintaining currency deposits or making currency purchases or

exchanges.

As shown above, present application describes how to synthesize a swap transaction using the features as described in the present application. It does not contemplate removing the characteristics of decentralized digital currencies that afford the aforementioned features as alleged by the Office Action. Implementing the benefits of the present application would not be possible using conventional transfer mechanisms, which all involve third party intermediaries, as described by Rosen, who temporarily control disposition of transfers. That is, the present application implemented on the decentralized digital currencies affords transactions between devices where no intermediary has an opportunity to behave badly or incompetently.

In contrast to amended **Claim 24**, not only Rosen fails to teach or suggest a method for processing a transaction implemented on decentralized digital currencies, but also *teaches away* the claimed method implemented on the decentralized digital currencies because Rosen identifies intermediaries who store and control currency (value) as agents or intermediaries or promissories. For example, Rosen describes various scenarios, all of which involve such controlling intermediaries like deposit banks, correspondent banks, participating banks, issuing banks, and clearing banks, see Rosen, at paragraph [0026] as reproduced below:

> [0026] To achieve the foregoing, and other objects, the method and apparatus of the present invention employ a preferred embodiment in the form of an electronic-monetary system having (1) banks or financial institutions that are coupled to a money generator device for generating and issuing to subscribing customers electronic money including electronic currency backed by demand deposits and electronic credit authorizations; (2) correspondent banks that accept and distribute the electronic money; (3) a plurality of transaction devices that are used by subscribers for storing electronic money, for performing money transactions with the on-line systems of the participating banks or for exchanging electronic money with other like transaction devices in off-line transactions; (4) teller devices, associated with the issuing and correspondent banks, for process handling and interfacing the transaction devices to the issuing and correspondent banks, and for interfacing between the issuing and correspondent banks themselves; (5) a clearing bank for balancing the electronic money accounts of the

> different issuing banks; (6) a data communications network for providing communications services to all components of the system; and (7) a security arrangement for maintaining the integrity of the system, and for detecting counterfeiting and tampering within the system.

A rogue intermediary in Rosen could abscond with funds in the middle of effecting a transfer. No configuration is described or suggested anywhere in Rosen that avoids the above vulnerability.

Further, Rosen describes mechanisms using cryptography managed by a **central authority** for the sole purpose of authentication (see Rosen, paragraph [0191], "This application provides each money module with the ability to check the digital signature for authenticity"). That is, the cryptography as described by Rosen is not used to effect transactions as recited in **Claim 24**. As discussed above, Rosen does not describe a means by which a transaction can be conducted without using intermediaries who control disposition.

In contrast to Rosen, because critical features of claimed *decentralized digital currencies* afford the facilitator's participation without allowing that the computer device to control dispositions, the present application does not suffer from the vulnerability caused by the intermediaries who control disposition.

Furthermore, Feigelson does not compensate for the above deficiencies of Rosen, and it is also submitted that there is no motivation to one of ordinary skill in the art to combine Rosen and Feigelson as proposed by the Office Action.

Feigelson describes encoding one's asymmetric key pair for use with a decentralized digital currency in multiple, removable layers on a wallet-sized card referred to throughout the application as a "bank card" (see Feigelson, paragraph [0077]). Feigelson further describes transferring decentralized digital currencies between keys on cards and keys not on cards on the same digital (sometimes referred to as "convert[ing]" bitcoins spendable by keys encoded in the plastic cards to bitcoins spendable by other keys, see Feigelson, paragraph [0078]). Nowhere does Feigelson describe nor even suggest how a

plastic card holder would construct a chain of transactions as claimed to adapt those cards for use in the conventional value transfer using intermediaries of Rosen much less while avoiding the aforementioned vulnerabilities of using the intermediaries as described by Rosen. Instead, Feigelson teaches away from the above combination with Rosen by contrasting the limitations of conventional transfer networks (like PayPal) to accommodate the benefits derived from Feigelson, see Feigelson, paragraphs [0018]-[0019] as reproduced below (emphasis added):

> [0018] ***Because of this practical inability to exchange digital stores-of-value physically without a risk that the secrecy of the stored information has been compromised somewhere in the chain of possession***, the predominant mechanism for utilizing value obtained in a digital transaction in a physical transaction or vice versa has been to exchange the store-of-value obtained in one realm for a different store-of-value better suited for the other realm. ***For example, to use value obtained in a digital transaction in a physical transaction (for example, to buy a meal at a restaurant), a user of the Paypal® digital payment service would transfer a balance of currency held in his Paypal account to his bank account and then withdraw physical bank notes from his bank.***
>
> [0019] For users who transact in both the digital and physical realms, there would be an advantage in having a payment system that functioned similarly in both digital and physical forms. If a digital store-of-value could be converted to an offline token that paralleled the digital form of the digital store-of-value, the complexity of the transitions between digital and physical transactions could be reduced. Such a token may allow users to convert their physical stores-of-value to digital form without the hassle or expense of any intermediary or third party. ***For example, where the user of the Paypal service must deposit paper money in a bank to transfer value to a Paypal account***, a holder of such a token could transfer the value for immediate digital use with only the help of simple software.

Based on the descriptions by Feigelson, any benefits derived from Feigelson require [decentralized] digital currencies to be effective. It is respectfully submitted that the proposed combination of Rosen and Feigelson would impermissibly render Feigelson unsatisfactory for its intended purpose because all benefits derived from Feigelson are lost when moving from tokens as described by Feigelson to conventional forms of account as described by Rosen. There is no way to

combine Feigelson with Rosen that retains the advantages of Feigelson's disclosure. Therefore, modifying Feigelson by adding features described in Rosen would impermissibly render Feigelson unsatisfactory for its intended purpose of providing security features for the physical devices that carry values. Moreover, the proposed modification would impermissibly change the principle of operation of Feigelson.

Accordingly, it is respectfully submitted that one of ordinary skill in the art would not have been motivated to combine Rosen and Feigelson as suggested in the Office Action because the proposed combination, under MPEP § 2143.01(V) and MPEP 2143.01(VI), cannot render the reference unsatisfactory for its intended purpose, and the proposed modification cannot change the principle of operation of a reference.

Additionally, the proposed combination of the cited references fail to teach or suggest "***broadcasting, via the transfer mechanism comprising the decentralized digital currency, the complete transaction record to the computing device, the first client device, and the second client device for verifying and effecting the transaction; observing an external state; and effecting the transaction when an action by at least two of the computing device, the first client device, or the second client device is detected based on the observed external state.***," as recited in amended **Claim 24**.

Further still, for at least the same reasons that independent **Claim 24** is patentable over the cited reference, it is respectfully submitted that **Claims 1 and 12** are also patentable, to the extent that **Claims 1 and 12** recite similar features as **Claim 24**. Accordingly, for at least the reasons set forth above regarding **Claim 24**, it is respectfully submitted that Rosen and Feigelson, either alone or in combination, fails to teach or suggest all the features of **Claims 1 and 12**; and, therefore, it is respectfully requested that the rejection to independent **Claims 1, 12, and 24** be reconsidered and withdrawn.

Dependent **Claims 3-6, 9, 15-17, 20, 23, 26, 28, 29, 31 and 32** depend, directly or indirectly, from independent **Claims 1, 12 and 24**, respectively. Accordingly, the dependent claims are allowable over

the cited references at least by virtue of their dependency from independent **Claims 1, 12 and 24**, as well as the other features recited therein. It is therefore respectfully requested that rejection to **Claims 3-6, 9, 15-17, 20, 23, 26, 28, 29, 31 and 32** under 35 U.S.C. § 103 be reconsidered and withdrawn.

CONCLUSION

It is respectfully submitted that the other references in the record do not compensate for the deficiencies of the references utilized in rejecting the pending claims.

It should also be noted that although arguments have been presented with respect to certain claims herein, the recited subject matter as well as various other subject matter and/or combinations of subject matter may be patentable for other reasons. Further, the failure to address any statement by the Examiner herein should not be interpreted as acquiescence or agreement with such statement. Applicant expressly reserves the right to set forth additional and/or alternative reasons for patentability and/or allowance with the present Application or in any other future proceeding, and to rebut any statement presented by the Examiner in this or other papers during prosecution of the present Application.

All objections and rejections having been addressed, it is respectfully submitted that the present application is in condition for allowance, and therefore issuance of a Notice to that effect is earnestly solicited.

Respectfully submitted,

Brundidge & Stanger, PC

Dated: December 8, 2020

/Misung Lee/
Misung Lee
Reg. No. 78,307

Electronic Patent Application Fee Transmittal

Application Number:	15309612
Filing Date:	08-Nov-2016
Title of Invention:	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers
First Named Inventor/Applicant Name:	Reginald Middleton
Filer:	Misung Lee/Juel Clyne
Attorney Docket Number:	4675.1002BS

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 $0 paid	2253	1	740	740
Miscellaneous:				
			Total in USD ($)	**740**

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. 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	~~2626.P100.US~~ 4675.1002BS
	Application Number	15/309,612
Title of Invention	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers	

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
	Reginald		Middleton	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Brooklyn	State/Province	NY	Country of Residence	US

Mailing Address of Inventor:

Address 1	195 Argyle Road		
Address 2			
City	Brooklyn	State/Province	NY
Postal Code	11218	Country	US

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Matthew		Bogosian	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Anacortes	State/Province	WA	Country of Residence	US

Mailing Address of Inventor:

Address 1	5007 Totem Trl		
Address 2			
City	Anacortes	State/Province	WA
Postal Code	98221	Country	US

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).

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. 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	~~2626.P100.US~~ 4675.1002BS
	Application Number	15/309,612
Title of Invention	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers	

☐ An Address is being provided for the correspondence Information of this application.			
Customer Number	~~115238~~ 86636		
Email Address	mail@brundidge-slanger.com	Add Email	Remove Email

Application Information:

Title of the Invention	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers		
Attorney Docket Number	~~2626.P100.US~~ 4675.1002BS	**Small Entity Status Claimed** ☒	
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	16	**Suggested Figure for Publication (if any)**	1

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.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	~~115238~~ 86636		

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	~~2626.P100.US~~ 4675.1002BS
	Application Number	15/309,612
Title of Invention	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers	

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)
~~PCT/US15/29196~~ 15/309,612	a 371 of international	PCT/US15/29196	2015-05-05
Prior Application Status	~~Pending~~ Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
~~61/990795~~ PCT/US15/29196	Claims benefit of provisional	61/990,795	2014-05-09

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.

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)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button.

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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	~~2626.P100.US~~ 4675.1002BS
	Application Number	15/309,612
Title of Invention	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers	

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 (11-15)
Approved for use through 04/30/2017. 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	~~2626.P100.US~~ 4675.1002BS
	Application Number	15/309,612
Title of Invention	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers	

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

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	~~Veritaseum, Inc.~~ Reginald Middleton

Mailing Address Information For Applicant:

Address 1	195 Argyle Road		
Address 2			
City	Brooklyn	**State/Province**	NY
Country	US	Postal Code	11218
Phone Number	718-407-4756	Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button.

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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	~~2626.P100.US~~ 4675 1002BS
	Application Number	15/309,612
Title of Invention	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers	

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.

If the Assignee or Non-Applicant Assignee is an Organization check here. ☒

~~Organization~~ Name	Reginald Middleton

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1	195 Argyle Road		
Address 2			
City	Brooklyn	**State/Province**	NY
Country i	US	Postal Code	11218
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.

Signature:

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	~~/JohnNielsen53392/~~ /Misung Lee/			Date (YYYY-MM-DD)	~~2016-11-04~~ 2021-01-21
First Name	~~John~~ Misung	Last Name	~~Nielsen~~ Lee	Registration Number	~~53,392~~ 78,307

Additional Signature may be generated within this form by selecting the Add button.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. 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	~~2626.P100.US~~ 4675.1002BS
	Application Number	15/309,612
Title of Invention	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers	

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.**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application Serial No. 15/309,612
Filing Date ..... November 08, 2016
Confirmation No. 2321
Inventorship ..... Reginald Middleton
Group Art Unit 3685
Examiner ..... NIGH, JAMES D
Attorney Docket No. 4675.1002BS
Title: ..... Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers

REQUEST TO CORRECT APPLICATION DATA SHEET

To: Commissioner for Patents
Office of Initial Patent Examination
P.O. Box 1450
Alexandria, VA 22313-1450

January 21, 2021

From: Misung Lee
Customer No. 86636
Brundidge & Stanger, PC
1925 Ballenger Ave. Ste 560
Alexandria, VA 22314

Sir:

It is respectfully submitted herewith a corrected Application Date Sheet (ADS) to correctly list Applicant information as:

"~~Veritaseum, Inc.~~" to "Reginald Middleton"

A patent assignment (Reel/Frame: 049973/0680) indicating Reginald Middleton as an assignee was recorded on August 6, 2019 with the USPTO.

It is respectfully requested that a Corrected Filing Receipt be issued stating the correct Applicant information. Please charge any fees or credit any overpayment to Deposit Account No.: 50-4888.

Respectfully submitted,

/Misung Lee/
Misung Lee
Reg. No. 78,307

Electronic Acknowledgement Receipt

EFS ID:	41684825
Application Number:	15309612
International Application Number:	
Confirmation Number:	2321
Title of Invention:	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers
First Named Inventor/Applicant Name:	Reginald Middleton
Customer Number:	86636
Filer:	Misung Lee/Juel Clyne
Filer Authorized By:	Misung Lee
Attorney Docket Number:	4675.1002BS
Receipt Date:	21-JAN-2021
Filing Date:	08-NOV-2016
Time Stamp:	09:53:48
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	Application Data Sheet	4675_Corrected_ADS_Response.pdf	38976 029d8d806e0da70b1b71040fcb62c6a36ea57aeb	no	1

Warnings:

Information:					
This is not an USPTO supplied ADS fillable form					
2	Application Data Sheet	4675_CorrectedADS.pdf	407803 fdb095d45da121174256ab32be1ded73e5bef9e8	no	7
Warnings:					
Information:					
This is not an USPTO supplied ADS fillable form					
			Total Files Size (in bytes):	446779	

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.

Notice of References Cited	Application/Control No. 15/309,612	Applicant(s)/Patent Under Reexamination Middleton et al.	
	Examiner JAMES D NIGH	Art Unit 3685	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-20130166455-A1	06-2013	Feigelson; Douglas	G06Q30/06	705/64
*	B	US-20030070080-A1	04-2003	Rosen, Sholom S.	G06Q20/06	713/187
*	C	US-20150287026-A1	10-2015	Yang; Danny	G06Q20/06	705/69
*	D	US-20090025087-A1	01-2009	Peirson, JR.; William Howard	G06Q10/00	726/27
*	E	US-20100138659-A1	06-2010	CARMICHAEL; PAT	H04L9/3263	713/170
*	F	US-20090030768-A1	01-2009	Ginter; Karl L.	G06Q20/04	705/39
*	G	US-7587369-B2	09-2009	Ginter; Karl L.	G06Q20/02	705/75
	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.

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.
15/309,612	11/08/2016	Reginald Middleton	4675.1002BS	2321

86636 7590 01/27/2021

BRUNDIDGE & STANGER, P.C.
1925 BALLENGER AVENUE, STE. 560
ALEXANDRIA, VA 22314

EXAMINER	
NIGH, JAMES D	

ART UNIT	PAPER NUMBER
3685	

MAIL DATE	DELIVERY MODE
01/27/2021	PAPER

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.

Office Action Summary	Application No. 15/309,612	Applicant(s) Middleton et al.	
	Examiner JAMES D NIGH	Art Unit 3685	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 December 8, 2020.

☐ 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) 1,3-6,9,12,15-17,20,23-24,26,28-29 and 31-32 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) 1,3-6,9,12,15-17,20,23-24,26,28-29 and 31-32 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: _____.

DETAILED ACTION

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.

Claim Status

2. As of the Office Action dated June 8, 2020 claims 1, 3-6, 9, 12, 15-17, 20, 23-24, 26, 28-29 and 31 were pending and claims 1, 3-6, 9, 12, 15-17, 20, 23-24, 26, 28-29 and 31 stood rejected. Claims 1, 3-6, 9, 12, 15-17, 20, 23-24, 26, 28-29 and 31 have been amended. Claim 32 has been added. No claims have been cancelled. Claims 1, 3-6, 9, 12, 15-17, 20, 23-24, 26, 28-29 and 31-32 are therefore currently pending and are presented for examination on the merits.

Response to Arguments

3. Applicant's argument with regard to the 35 U.S.C. § 101 rejection of claims 1, 3-6, 9, 12, 15-17, 20, 23-24, 26, 28, 29 and 31-32 has been fully considered but is not persuasive. Applicant argues that claim 24 (which Applicant has indicated is also representing claims 1 and 12) does not fall within one of the groupings of abstract ideas identified by the 2019 PEG (argument beginning on page 22 of remarks concluding on page 26). Applicant states that claim 24 is "…directed to a specific method for enabling increased security for either party entering into the transaction via the decentralized digital currency of the transfer mechanism, without requiring expensive tamper-proof electronic units" (remarks at page 25). Applicant did not point to any portion of the written disclosure that would indicate that the inventors viewed their invention as solving a security problem however even if the written record actually reflected that the

invention was directed towards some form of security enhancement the argument itself only suggests that some form of increased business security was desired and that no technological solution is being employed to achieve the security. Applicant also offers an argument that decentralization somehow takes the claim out of the realm of a fundamental economic practice. The problem with this argument is that decentralization is also an abstract concept and simply adding layers of abstraction to an abstract idea does not make the claim any less abstract. Therefore Applicant has failed to show any clear error on the part of the examiner in holding that the claim is ineligible under Prong One of Step 2A.

4. Applicant then argues that a practical application is present under Prong Two of Step 2A (remarks at pages 26-34). Applicant attempts to compare the claimed invention to examples from the 2019 PEG in order to establish that a practical application of the abstract idea is present in the claim. Applicant alleges that the claim is similar to Example 40 from the 2019 PEG involving network monitoring and states that the operation of "effecting of the complete disbursement transaction to when an action by at least two of the network participants is detected based on the observed external state" (remarks at page 28). The problem with this argument is that the observed state, per the written disclosure at paragraph 31 is that the external state is exemplified by the language "… the relative value of certain financial instruments at a specific time" which clearly is a form of business event and not a technological event such as the one in the claim from example 40. Similarly Applicant's remark that the claimed invention "avoids involvement of expensive third party intermediaries" also has to be viewed if anything as a business improvement but certainly is not a technological

improvement that would form a practical application under Prong Two of Step 2A as monitoring the value of financial instruments is another abstract idea. Similarly with regard to Applicant's allegation that the claim is similar to Example 41 from the 2019 PEG it is noted that Applicant states in remarks that "…Claim 24 is directed to an improvements (sic) in processing transaction technology, particularly, via a transfer mechanism comprising a decentralized digital currency with enhanced security". Again the "enhanced security" feature Applicant is relying upon in argument is not discussed in the written disclosure however it is also noted that enhanced security in a business or economic transaction is an abstract idea itself and cannot be viewed under Prong Two of Step 2A as the basis for forming a practical application under the 2019 PEG. Similarly having a transaction "validated by a number of participants" (remarks at pages 29-30) is also an abstract idea that cannot serve as the basis for a practical application under the 2019 PEG. With regard to Applicant's remarks regarding a "transfer mechanism comprising a decentralized digital currency" (remarks at pages 31-34) are directed not towards any technological improvements but merely those that involve business arrangements and again a decentralized currency is another abstract idea. A decentralized currency is not something that is unique to the internet world as barter economies could be described as decentralized and grains and precious metals which have long been used in economic exchange have no central issuing authority. Applicant's argument discusses a swap transaction involving cryptocurrency but produces no reasoning as to why such a transaction incorporates any technological improvement to the functioning of an underlying computer. The arguments are employing any of the rationales from the 2019 PEG for determining whether a practical

application is present and merely provide a conclusory argument that a practical application is present. However as no showing of clear error on the part of the Examiner has been made this argument is unpersuasive.

5. Applicant's further argument (pages 34-37 of remarks) with regard to the present rejection under section 101 that the claims amount to significantly more than the abstract idea under Step 2B has been fully considered but is not persuasive. The arguments are substantially similar to those presented regarding Prong Two of Step 2A and Examiner does not see where Applicant has actually pointed to any technological improvement that is taking place but instead is pointing to an improvement that is related to conducting business using the claimed invention. However an improvement that is directed entirely towards a business objective must be viewed as being part of the abstract idea itself and does not serve under Step 2B to form something that can be viewed as contributing significantly more to the claim then the abstract idea itself. Therefore this argument is also unpersuasive.

6. Applicant's argument with regard to the 35 U.S.C. § 112 (b) rejection of claims 1, 3-6 and 9 has been fully considered and is persuasive. Accordingly the rejection will be withdrawn.

7. Applicant's argument with regard to the 35 U.S.C. § 103 rejection of claims 1, 3-6, 9, 12, 15-17, 20, 23-24, 26, 28, 29 and 31-32 as being unpatentable over Rosen (U.S. Patent Publication 2003/0070080) in view of Feigelson (U.S. Patent Publication 2013/0166455) has been fully considered but is moot in view of the new grounds of rejection. However Examiner would reiterate that as the claim is directed towards a role of an intermediary that there is nothing in the claim that would alter the function of the

intermediary based on whether a centralized or decentralized currency were being used and Applicant has presented nothing more than a conclusory argument. Furthermore there is nothing within the Rosen reference that disparages the use of a decentralized currency and in order to "teach away" from the claimed invention the reference would have to make a statement to the effect that precludes or disparages the use of cryptocurrency (*In re Fulton*, 391 F.3d 1195, 1201, 73 USPQ2d 1141, 1146 (Fed. Cir. 2004), MPEP § 2123, 2141.02 (VI)). Without such a statement present in the Rosen reference itself the allegation that Rosen "teaches away" from the use of decentralized currency must be held as unpersuasive.

Claim Rejections - 35 USC § 101

8. 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.

9. Claims 1, 3-6, 9, 12, 15-17, 20, 23-24, 26, 28, 29 and 31-32 are rejected under 35 U.S.C. 101 because the claimed invention is directed to an abstract idea without significantly more.

10. Claim 1 recites a device and therefore meets Step 1 of the 2019 Revised Patent Subject Matter Eligibility Guidance as it can be viewed as a machine which falls within one of the four categories of statutory subject matter. Claim 1 recites as follows:

1. (Currently Amended) A computing device for processing a transaction between a first client device and a second client device via a transfer mechanism, the transfer mechanism comprising a decentralized digital currency, the computing device comprising:

a memory for storing a first asymmetric key pair, the first asymmetric key pair comprising a first private key and a first public key;

a network interface for receiving terms, the terms comprising:

at least one of a first principal data or a second principal data;

a reference to at least one of a first data source or a second data source; and

an expiration timestamp;

a computer processor coupled to the memory and the network interface, the first computer processor configured to:

read the first private key from the memory;

compute a first cryptographic signature from the first private key;

create an inchoate data record comprising:

a commit input for receiving a commit data from a commit transaction;

one or more output data obtained from at least one of the first principal data or the second principal data, and a value data from at least one of the first data source or the second data source; and

the first cryptographic signature; and

publish the inchoate data record to at least one of the first client device and the second client device;

wherein the inchoate data record is used by at least one of the first client device or the second client device to create a complete data record and to create a transaction by submitting the complete data record to the transfer mechanism,

wherein the transfer mechanism comprises the decentralized digital currency that is accessible via a computer network by the computing device, the first client device,

and the second client device, respectively, and the complete data record is broadcast, via the transfer mechanism to the computing device, the first client device, and the second client device for verifying and effecting the transaction,

wherein an external state is observed by each of the computing device, the first client device, and the second client device and the transaction is effected when an action by at least two of the computing device, the first client device, or the second client device is detected based on the observed external state.

The claim is analyzed under prong one, step 2A in order to determine if the claim is directed towards a judicial exception. The claim recites in the preamble that it is processing a transaction between a first client device and a second client device using a transfer mechanism comprising a decentralized digital currency. Asymmetric key pairs are used and terms are received comprising a first or second principal data, a reference to one of two data sources and an expiration time stamp. Data is obtained from at least one of two principal data and value data from at least one of two data sources. A private key is retrieved and is used to compute a cryptographic signature. A data record is then formed by receiving commit data, one or more output data and the computed cryptographic signature and the record is then published to at least one of a first and second client device. The claim falls within two groupings of abstract ideas involving the organizing of human activity as indicated in the 2019 Revised Patent Subject Matter Eligibility Guidance, one of which is the processing of a payment between two parties which falls under the category of a fundamental economic practice. As the claim also recites that the transaction requires particular signatures of the intermediary and the first or second client device the claim can also be viewed as falling within the category of a

commercial/legal interaction involving a contract involving terms including principal data, references to data sources and expiration of the terms i.e. requiring that the contract be consummated within a specified period of time that result in the creation of a disbursement transaction record including amounts, values, signatures and commitment inputs that are then published to both parties to the contract. With regard to the observing of an external state and the affecting of the transaction based on the observed state this can also be viewed as a mental process that is capable of being performed by a human being via observation and evaluation. The disclosure itself recites at paragraph 108 that "The invention pertains to agreements among distinct parties that contemplate transfer of title to property, as well as any industry where that may be of value or importance" and clearly falls within the grouping of commercial/legal interactions under the groupings. The encryption is being claimed at a generally high level and only serves to add a mathematical relationship to the claim as it is directed towards another one of the groupings in the 2019 PEG. Many of the operations can also be performed by human beings using pen and paper such as obtaining terms, creating records and performing transactions. Therefore under the analysis made under prong one of step 2A the claim is determined to be ineligible.

The analysis then proceeds to prong two of step 2A where an analysis is performed in order to determine whether the claim recites additional elements that integrate the abstract idea into a practical application of the abstract idea. Integrating the claim into a practical application requires an additional element or a combination of additional elements in the claim to apply, rely on, or use the judicial exception in a manner that imposes a meaningful limit on the judicial exception, such that the claim is

more than a drafting effort designed to monopolize the exception. The structural elements in the claim include the memory of the claimed device, a network interface and a processor. The claim also recites that the device possesses the capability of encryption by taking a private key and computing a cryptographic signature. In reviewing the written disclosure at paragraphs 52-53, 106 and 113 the processor, memory and network interface are described in a manner that includes no technological improvement to the functioning of the processor and only describes a particular technological environment for which an intermediary described in paragraph 113 as a "facilitator" is linked. With regard to the encryption capabilities no particular algorithm for computing a signature is described in the written disclosure beyond the recitations at pages 17, 18 and 28 that in order to consummate a transaction that a plurality of signatures are required and the function is described at a generally high level by the written disclosure such that in the broadest reasonable interpretation the claim scope encompasses encryption that could be performed by human beings. Even if a computer calculation of the signature were inferred from the claim the written disclosure relies on prior art signature calculation mechanisms such as multisignature transactions (see footnote 2 of page 4 of the written disclosure) or P2SH (97 and 104 of the written disclosure) and therefore do not constitute any technological improvement to the functioning of the computer itself. While the claim scope is limited in scope to the computing device acting as a facilitator or intermediary Examiner will also consider the participation of the two client devices. The first and second client devices are simply serving as proxies for human participants and are being recited at a generally high level. As pointed out paragraphs 52-53 and 106 of the written disclosure are directed towards

a generic computing environment that include no technological improvement to the functioning of any particular computer and paragraph 110 in describing the client also describes a generic computing device with no technological improvement. If the combination of facilitator and two clients are considered there is no meaningful technological contribution being made as the facilitator and clients merely represent the computer equivalents of two parties to a contract in which an intermediary is used and therefore the combination as a whole is merely a mechanism for linking the abstract idea to a particular technological environment. Therefore under prong two of Step 2A no practical application of the abstract idea is present in the claim and the result of the analysis is that the claim is still ineligible.

Dependent claims 3-6 and 9 recite the same elements as claim 1 inclusive of different data but utilize the same structural components and signature computation present in claim 1. Therefore under both prongs one and two of Step 2A these limitations only serve to add additional layers of abstraction to the abstract idea of claim 1 and therefore under prongs one and two of step 2A are also found to be ineligible.

The analysis proceeds to step 2B of the 2019 Revised Patent Subject Matter Eligibility Guidance. The claim recites structural elements in the claim including the memory of the claimed device, a network interface and a processor. The claim also recites that the device possesses the capability of encryption by taking a private key and computing a cryptographic signature. In reviewing the written disclosure at paragraphs 52-53, 106 and 113 the processor, memory and network interface are described in a manner that includes no technological improvement to the functioning of the processor and only describes a particular technological environment for which an

intermediary described in paragraph 113 as a “facilitator” is linked. With regard to the encryption capabilities no particular algorithm for computing a signature is described in the written disclosure beyond the recitations at pages 17, 18 and 28 that in order to consummate a transaction that a plurality of signatures are required and the function is described at a generally high level by the written disclosure such that in the broadest reasonable interpretation the claim scope encompasses encryption that could be performed by human beings. Even if a computer calculation of the signature were inferred from the claim the written disclosure relies on prior art signature calculation mechanisms such as multisignature transactions (see footnote 2 of page 4 of the written disclosure) or P2SH (97 and 104 of the written disclosure) and therefore do not constitute any technological improvement to the functioning of the computer itself. While the claim scope is limited in scope to the device acting as a facilitator or intermediary Examiner will also consider the two client’s participation. The first client device and second client are claimed at a generally high level and only serve as proxies for the entities engaged in the transaction. As pointed out paragraphs 52-53 and 106 of the written disclosure are directed towards a generic computing environment that include no technological improvement to the functioning of any particular computer and paragraph 110 in describing the client also describes a generic computing device with no technological improvement. If the combination of facilitator and two clients are considered there is no meaningful technological contribution being made as the facilitator and clients merely represent the computer equivalents of two parties to a contract in which an intermediary is used and therefore the combination as a whole is merely a mechanism for linking the abstract idea to a particular technological

environment. No technological improvement is recited to the recited device, nor does the combination of device and two clients serve to form an ordered combination of elements that results in any technological improvement. It is abundantly clear that the claim does not involve any ordered combination of elements as the recited device does not utilize any special properties of a network or distributed computing in order to gain any technological improvement and merely are directed towards a centralized, "one-size-fits-all" technological implementation and the clients merely serve as representatives of human counterparts engaging in a contract (*BASCOM Glob. Internet Servs. v. AT&T Mobility, LLC*, 119 USPQ2d 1236 (Fed. Cir. 2016)). It is also clear that no similarity is present with regard to *McRO* (*McRO, Inc. v. Bandai Namco Games Am. Inc.*, 120 USPQ2d 1091 (Fed. Cir. 2016)) as the process applied in McRO which involved the evaluation of a plurality of subsequences of phonemes in order to set morph weights and was a process that was not previously used by human beings in performing lip synchronization between the animated characters and the reproduced sounds. While *McRO* acknowledged that human beings could perform the operations recited in the steps it was also clear that human beings had never previously acted in such a manner, particularly as it applied to the evaluation of subsequences of phonemes in order to set the morph weights. However in the instant claims the recited operations of transferring payments and utilizing trusted intermediaries in making a payment are all operations that have previously been done by human beings in the same manner being claimed. It is also clear that there is no similarity to *DDR Holdings* (*DDR Holdings, LLC v. Hotels.com, LP*, 113 USPQ2d 1097 (Fed. Cir. 2014)) as there is nothing in the claims themselves or even in the written description to explicitly state or

even implicitly suggest that the claims involve anything more than generic computer operations. It is also clear that there is no similarity to *Enfish* (*Enfish, LLC v. Microsoft Corp.*, 118 USPQ2d 1684 (Fed. Cir. 2016)) because nothing within the claim or the four corners of the written description provides any teaching or suggestion of an improved computer algorithm for analyzing data such as the self-referential table of *Enfish* that brings about an improvement to the computer itself where *Enfish* taught that the claimed invention brought about "increased flexibility, faster search times, and smaller memory requirements" (*Enfish* at 1690). There is also no technological improvement being made to any external technology (*Diamond v. Diehr*, 450 U.S. 175, 184 (1981)). The written disclosure at paragraphs 52-53, 106, 110 and 113 describe only the use of a generic unimproved computing environment and describes the elements in a manner that indicates that the additional elements are sufficiently well-known that the specification does not need to describe the particulars of such additional elements to satisfy 35 U.S.C. §112 (a) ("In other words, the claims in *Diehr* were patent eligible because they improved an existing technological process, not because they were implemented on a computer", *Alice* at 1983). Therefore it is clear that no inventive concept is present sufficient to confer eligibility in light of the fact that the claims are clearly directed towards an abstract idea. Therefore claims 1, 3-6 and 9 are rejected under 35 U.S.C. § 101 as being directed towards ineligible subject matter.

11. Claim 12 recites a system and therefore meets Step 1 of the 2019 Revised Patent Subject Matter Eligibility Guidance as it can be viewed as a product which falls within one of the four categories of statutory subject matter. Claim 12 recites as follows:

12. (Currently Amended) A system for processing a transaction between a first client device and a second client device via a transfer mechanism, the system comprising a computing device, the first client device, and the second client device, and the transfer mechanism; the computing device comprising:

a first memory comprising for storing a first asymmetric key pair, the first asymmetric key pair comprising a first private key and a first public key;

a first network interface for receiving terms, the terms comprising:

at least one of a first principal data or a second principal data;

a reference to at least one of a first data source or a second data source; and

an expiration timestamp; and

a first computer processor coupled to the first memory and the first network interface, the first computer processor configured to:

read the first private key from the first key pair sector;

compute a first cryptographic signature from the first private key;

create an inchoate data record comprising:

a commit input for receiving a commit data from a commit transaction;

one or more outputs obtained from at least one of the first principal data or the second principal data, and a value data from at least one of the first data source or the second data source; and

the first cryptographic signature; and

publish the inchoate data record to at least one of the first client device and the second client device;

the first client device comprising:

a second memory for storing a second asymmetric key pair, the second asymmetric key pair comprising a second private key and a second public key;

a second network interface; and

a second computer processor coupled to the second memory and the second network interface, the second computer processor configured to; read the second private key from the memory;

read the inchoate data record;

compute a second cryptographic signature from the second private key;

create a complete data record comprising:

the commit input;

the output data;

the first cryptographic signature; and

the second cryptographic signature; and

create a transaction by submitting the complete data record to the transfer mechanism; and

the second client comprising:

a third memory for storing a third asymmetric key pair, the third asymmetric key pair comprising a third private key and a third public key;

a third network interface; and

a third computer processor coupled to the third memory and the third network interface, the third computer processor configured to read the third private key from the third memory; and

the transfer mechanism comprising the decentralized digital currency that is accessible via a computer network by the computing device, the first client device, and the second client device, respectively, the transfer mechanism configured to broadcast the complete data record to the computer device, the first client device, and the second client device for verifying and effecting the transaction,

wherein an external state is observed by each of the computer device, the first client device, and the second client device, and the transaction is effected when an action by at least two of the computer device, the first client device, or the second client device is detected based on the observed external state.

The claim is analyzed under prong one, step 2A in order to determine if the claim is directed towards a judicial exception. The claim recites in the preamble that it is directed towards a transaction between a first client device and a second client device via a transfer mechanism which is later described as being a decentralized digital currency. Asymmetric key pairs are used and terms are received comprising a first or second principal data, a reference to one of two data sources and an expiration time stamp. A private key is retrieved and is used to compute a cryptographic signature. A transaction record is then formed by receiving a commit input, one or more outputs and a value data and the computed cryptographic signature and the record is then published to at least one of a first and second client. The system includes an intermediary device for facilitating a value transfer between a first client device and a second client device. The first client reads a second private key and the transaction record and computes a second cryptographic signature from the second private key and creates a complete disbursement record comprising the commit input, the output data and the first and

second cryptographic signatures and creates a transaction by submitting the complete data record to the transfer mechanism. The second client is recited as storing public and private keys and reading the private key. The claim falls within two groupings of abstract ideas involving the organizing of human activity as indicated in the 2019 Revised Patent Subject Matter Eligibility Guidance, one of which is the processing of a payment between two parties which falls under the category of a fundamental economic practice. As the claim also recites that the transaction requires particular signatures of the intermediary and the first client the claim can also be viewed as falling within the category of a commercial/legal interaction involving a contract involving terms including principal amounts, references to data sources and expiration of the terms i.e. requiring that the contract be consummated within a specified period of time that result in the creation of a disbursement transaction record including amounts, values, signatures and commitment inputs that are then published to both parties to the contract. The disclosure itself recites at paragraph 108 that “The invention pertains to agreements among distinct parties that contemplate transfer of title to property, as well as any industry where that may be of value or importance” and clearly falls within the grouping of commercial/legal interactions under the groupings. The encryption is being claimed at a generally high level and only serves to add a mathematical relationship to the claim as it is directed towards another one of the groupings in the 2019 PEG. Many of the operations can also be performed by human beings using pen and paper such as obtaining terms, creating records and performing transactions. Therefore under the analysis made under prong one of step 2A the claim is determined to be ineligible.

The analysis then proceeds to prong two of step 2A where an analysis is performed in order to determine whether the claim recites additional elements that integrate the abstract idea into a practical application of the abstract idea. Integrating the claim into a practical application requires an additional element or a combination of additional elements in the claim to apply, rely on, or use the judicial exception in a manner that imposes a meaningful limit on the judicial exception, such that the claim is more than a drafting effort designed to monopolize the exception. The structural elements in the claim include the memory of the claimed computing device further including a network interface and a processor, the first client device including a memory, a network interface and a processor and a second client device including a memory, a network interface and a processor. The claim also recites that the computing device and the first client device possess the capability of encryption by taking a private key and computing a cryptographic signature. In reviewing the written disclosure at paragraphs 52-53, 106 and 113 the processor, memory and network interface of the facilitator device are described in a manner that includes no technological improvement to the functioning of the processor and only describes a particular technological environment for which an intermediary described in paragraph 113 as a “facilitator” is linked. With regard to the encryption capabilities no particular algorithm for computing a signature is described in the written disclosure beyond the recitations at pages 17, 18 and 28 that in order to consummate a transaction that a plurality of signatures are required and the function is described at a generally high level by the written disclosure such that in the broadest reasonable interpretation the claim scope encompasses encryption that could be performed by human beings. Even if a computer calculation of

the signature were inferred from the claim the written disclosure relies on prior art signature calculation mechanisms such as multisignature transactions (see footnote 2 of page 4 of the written disclosure) or P2SH (97 and 104 of the written disclosure) and therefore do not constitute any technological improvement to the functioning of the computer itself. With regard to the two client devices the first client device also comprises a memory, a network interface and a processor and is also performing a computation of a cryptographic signature using a private key. The second client device also comprises a memory, a network interface and a processor. As pointed out paragraphs 52-53 and 106 of the written disclosure are directed towards a generic computing environment that include no technological improvement to the functioning of any particular computer and paragraph 110 in describing the client also describes a generic computing device with no technological improvement. If the combination of facilitator and two clients are considered there is no meaningful technological contribution being made in the form of a combination of elements as the facilitator and clients merely represent the computer equivalents of two parties to a contract in which an intermediary is used and therefore the combination as a whole is merely a mechanism for linking the abstract idea to a particular technological environment. Therefore under prong two of Step 2A no practical application of the abstract idea is present in the claim and the result of the analysis is that the claim is still ineligible.

Dependent claims 15-17, 20 and 23 recite the same elements as claim 12 inclusive of different data but utilize the same structural components and signature computation present in claim 12. Therefore under both prongs one and two of Step 2A these limitations only serve to add additional layers of abstraction to the abstract idea of

claim 1 and therefore under prongs one and two of step 2A are also found to be ineligible.

The analysis proceeds to step 2B of the 2019 Revised Patent Subject Matter Eligibility Guidance. The claim recites structural elements in the claim including the memory of the claimed facilitator device further including a network interface and a processor and two client devices also including a memory, a network interface and a processor. The claim also recites that the computing device and the first client device possess the capability of encryption by taking a private key and computing a cryptographic signature. In reviewing the written disclosure at paragraphs 52-53, 106 and 113 the processor, memory and network interface are described in a manner that includes no technological improvement to the functioning of the processor and only describes a particular technological environment for which an intermediary described in paragraph 113 as a "facilitator" is linked. With regard to the encryption capabilities no particular algorithm for computing a signature is described in the written disclosure beyond the recitations at pages 17, 18 and 28 that in order to consummate a transaction that a plurality of signatures are required and the function is described at a generally high level by the written disclosure such that in the broadest reasonable interpretation the claim scope encompasses encryption that could be performed by human beings. Even if a computer calculation of the signature were inferred from the claim the written disclosure relies on prior art signature calculation mechanisms such as multisignature transactions (see footnote 2 of page 4 of the written disclosure) or P2SH (97 and 104 of the written disclosure) and therefore do not constitute any technological improvement to the functioning of the computer itself. The first client device also

comprises a memory, a network interface and a processor and is also performing a computation of a cryptographic signature using a private key. The second client device also comprises a memory, a network interface and a processor. As pointed out paragraphs 52-53 and 106 of the written disclosure are directed towards a generic computing environment that include no technological improvement to the functioning of any particular computer and paragraph 110 in describing the client also describes a generic computing device with no technological improvement. If the combination of facilitator and two clients are considered there is no meaningful technological contribution being made as the facilitator and clients merely represent the computer equivalents of two parties to a contract in which an intermediary is used and therefore the combination as a whole is merely a mechanism for linking the abstract idea to a particular technological environment. No technological improvement is recited to the recited computing device or the two client devices nor does the combination of device and two client devices serve to form an ordered combination of elements that results in any technological improvement. It is abundantly clear that the claim does not involve any ordered combination of elements as the recited facilitator device along with the two clients do not utilize any special properties of a network or distributed computing in order to gain any technological improvement and merely are directed towards a centralized, "one-size-fits-all" technological implementation and the clients merely serve as representatives of human counterparts engaging in a contract (*BASCOM Glob. Internet Servs. v. AT&T Mobility, LLC*, 119 USPQ2d 1236 (Fed. Cir. 2016)). It is also clear that no similarity is present with regard to *McRO* (*McRO, Inc. v. Bandai Namco Games Am. Inc.*, 120 USPQ2d 1091 (Fed. Cir. 2016)) as the process applied in McRO

which involved the evaluation of a plurality of subsequences of phonemes in order to set morph weights and was a process that was not previously used by human beings in performing lip synchronization between the animated characters and the reproduced sounds. While *McRO* acknowledged that human beings could perform the operations recited in the steps it was also clear that human beings had never previously acted in such a manner, particularly as it applied to the evaluation of subsequences of phonemes in order to set the morph weights. However in the instant claims the recited operations of transferring payments and utilizing trusted intermediaries in making a payment are all operations that have previously been done by human beings in the same manner being claimed. It is also clear that there is no similarity to *DDR Holdings* (*DDR Holdings, LLC v. Hotels.com, LP*, 113 USPQ2d 1097 (Fed. Cir. 2014)) as there is nothing in the claims themselves or even in the written description to explicitly state or even implicitly suggest that the claims involve anything more than generic computer operations. It is also clear that there is no similarity to *Enfish* (*Enfish, LLC v. Microsoft Corp.*, 118 USPQ2d 1684 (Fed. Cir. 2016)) because nothing within the claim or the four corners of the written description provides any teaching or suggestion of an improved computer algorithm for analyzing data such as the self-referential table of *Enfish* that brings about an improvement to the computer itself where *Enfish* taught that the claimed invention brought about "increased flexibility, faster search times, and smaller memory requirements" (*Enfish* at 1690). There is also no technological improvement being made to any external technology (*Diamond v. Diehr*, 450 U.S. 175, 184 (1981)). The written disclosure at paragraphs 52-53, 106, 110 and 113 describe only the use of a generic unimproved computing environment and describes the elements in a manner

that indicates that the additional elements are sufficiently well-known that the specification does not need to describe the particulars of such additional elements to satisfy 35 U.S.C. §112 (a) ("In other words, the claims in *Diehr* were patent eligible because they improved an existing technological process, not because they were implemented on a computer", *Alice* at 1983). Therefore it is clear that no inventive concept is present sufficient to confer eligibility in light of the fact that the claims are clearly directed towards an abstract idea. Therefore claims 12, 15-17, 20 and 23 are rejected under 35 U.S.C. § 101 as being directed towards ineligible subject matter.

12. Claim 24 recites a method and therefore meets Step 1 of the 2019 Revised Patent Subject Matter Eligibility Guidance as it can be viewed as a product which falls within one of the four categories of statutory subject matter. Claim 24 recites as follows:

24. (Currently Amended) A method for processing a transaction between a first client device and a second client device via a transfer mechanism, the transfer mechanism comprising a decentralized digital currency that is accessible via a computer network by a computer device, the first client device and the second client device, respectively, the method comprising:

storing a first asymmetric key pair in a first memory, the first asymmetric key pair comprising a first private key and a first public key;

storing a second asymmetric key pair a second memory, the second asymmetric key pair comprising a second private key and a second public key;

storing a third asymmetric key pair in the second memory, the third key pair comprising a third private key and a third public key;

storing a fourth asymmetric key pair in a third memory, the fourth asymmetric key pair comprising a fourth private key and a fourth public key;

transmitting terms from one of the first or second client device via a first network interface, the terms comprising:

at least one of a first principal data or a second principal data;

a reference to at least one of a first data source or a second data source; and

an expiration timestamp;

receiving the terms at the computer device via a second network interface;

reading the first private key from the first key pair sector;

computing a first cryptographic signature from the first private key;

creating a first principal transaction data record comprising:

a first principal output comprising the first principal data; and

the first cryptographic signature;

creating a first principal transaction by submitting the first principal transaction data record to the transfer mechanism;

reading the second private key from the second memory;

computing a second cryptographic signature from the second private key;

creating a commit transaction data record comprising:

a first principal input for receiving the first principal data from the first principal transaction;

a commit output comprising a commit data; and

the second cryptographic signature;

creating the commit transaction by submitting the commit transaction data record to the transfer mechanism;

retrieving a value data from the first data source;

reading the third private key from the second memory;

computing a third cryptographic signature from the second private key;

creating an inchoate data record comprising:

a commit input for receiving a commit data from the commit transaction;

one or more output data obtained from the at least one of the first principal data or the second principal data and the value from the first data source; and

the third cryptographic signature;

publishing the inchoate data record;

reading the inchoate data record;

reading the fourth private key from the third memory;

computing a fourth cryptographic signature from the fourth private key;

creating a complete data record comprising:

the commit input;

the one or more output data;

the third cryptographic signature; and

the fourth cryptographic signature;

creating a transaction by submitting the complete data record to the transfer mechanism;

broadcasting, via the transfer mechanism comprising the decentralized digital currency, the complete transaction record to the computing device, the first client device, and the second client device for verifying and effecting the transaction;

observing an external state; and

effecting the transaction when an action by at least two of the computing device, the first client device, or the second client device is detected based on the observed external state.

The claim is analyzed under prong one, step 2A in order to determine if the claim is directed towards a judicial exception. The claim recites in the preamble that it is directed towards processing a transaction between a first client device and a second device. Four asymmetric key pairs are first stored. The first or second client device sends terms to a device including principal data, reference to a data source and an expiration timestamp. The computing device receives the terms and then reads a private key and computes a cryptographic signature and then creates a first principal transaction data record comprising the first principal data and the cryptographic signature. The first principal transaction data is then submitted to the transfer mechanism. A second private key is read and a second cryptographic signature is computed from the second private key. A commit transaction data record is then created comprising a first principal input for receiving the first principal data, a commit output comprising a commit data and the second cryptographic signature. A value is retrieved, a third private key is read and a third cryptographic signature is computed using a second private key. An inchoate data record is then created comprising a commit input, one or more output data obtained from the first and/or second principal

data, the data source value and the third cryptographic signature. The inchoate data record is then published. The inchoate data record is then read. A fourth private key is read, a fourth cryptographic signature is computed and a complete disbursement transaction record is created comprising the commit input, one or more disbursement outputs and the third and fourth cryptographic signature. A transaction is then created by submitting the complete data record to the transfer mechanism. The transaction record is then broadcasted, an external state is observed and the transaction is effected when an action is detected by two of the three devices (computing device, first client device and/or second client device). The claim falls within two groupings of abstract ideas involving the organizing of human activity as indicated in the 2019 Revised Patent Subject Matter Eligibility Guidance, one of which is the processing of a payment between two parties which falls under the category of a fundamental economic practice. As the claim also recites that the transaction requires particular signatures of the intermediary and the first client the claim can also be viewed as falling within the category of a commercial/legal interaction involving a contract involving terms including principal amounts, references to data sources and expiration of the terms i.e. requiring that the contract be consummated within a specified period of time that result in the creation of a disbursement transaction record including amounts, values, signatures and commitment inputs that are then published to both parties to the contract. The disclosure itself recites at paragraph 108 that “The invention pertains to agreements among distinct parties that contemplate transfer of title to property, as well as any industry where that may be of value or importance” and clearly falls within the grouping of commercial/legal interactions under the groupings. The encryption is being claimed

at a generally high level and only serves to add a mathematical relationship to the claim as it is directed towards another one of the groupings in the 2019 PEG. Many of the operations can also be performed by human beings using pen and paper such as obtaining terms, creating records and performing transactions. Therefore under the analysis made under prong one of step 2A the claim is determined to be ineligible.

The analysis then proceeds to prong two of step 2A where an analysis is performed in order to determine whether the claim recites additional elements that integrate the abstract idea into a practical application of the abstract idea. Integrating the claim into a practical application requires an additional element or a combination of additional elements in the claim to apply, rely on, or use the judicial exception in a manner that imposes a meaningful limit on the judicial exception, such that the claim is more than a drafting effort designed to monopolize the exception. The structural elements in the claim are limited to what is described as a “transfer mechanism”, three memories and two network interfaces along with recitations of first and second clients in the preamble. The claim also recites the capability of encryption by taking a private key and computing a cryptographic signature. In reviewing the written disclosure at paragraphs 52-53, 106 and 113 the memory and network interface are described in a manner that includes no technological improvement to the functioning of the memory and network interface and only describes a particular technological environment for which an intermediary described in paragraph 113 as a “facilitator” is linked. With regard to the encryption capabilities no particular algorithm for computing a signature is described in the written disclosure beyond the recitations at pages 17, 18 and 28 that in order to consummate a transaction that a plurality of signatures are required and the

function is described at a generally high level by the written disclosure such that in the broadest reasonable interpretation the claim scope encompasses encryption that could be performed by human beings. Even if a computer calculation of the signature were inferred from the claim the written disclosure relies on prior art signature calculation mechanisms such as multisignature transactions (see footnote 2 of page 4 of the written disclosure) or P2SH (97 and 104 of the written disclosure) and therefore do not constitute any technological improvement to the functioning of the computer itself. With regard to the two clients paragraph 110 in describing the client also describes a generic computing device with no technological improvement. The transfer mechanism per paragraphs 53, 54 and 96 are not elements of physical structure but instead are protocols involving at least decentralized currency ("Where a decentralized digital currency [e.g., the Bitcoin protocol, the Ethereum protocol, or similar] *is used as the transfer mechanism*...", 96) but per paragraph 49 can also involve centralized currency and the broadest reasonable interpretation of the term transfer mechanism can be viewed as any form of monetary exchange scheme. If the combination of transfer mechanism, memory, network interfaces and two clients are considered there is no meaningful technological contribution being made in the form of a combination of elements as the transfer mechanism and clients merely represent the computer equivalents of two parties to a contract in which an intermediary is used through the network interfaces and therefore the combination as a whole is merely a mechanism for linking the abstract idea to a particular technological environment. Therefore under prong two of Step 2A no practical application of the abstract idea is present in the claim and the result of the analysis is that the claim is still ineligible.

Dependent claims 26, 28, 29, 31 and 32 recite the same elements as claim 24 inclusive of different data but utilize the same structural components and signature computation present in claim 24. Therefore under both prongs one and two of Step 2A these limitations only serve to add additional layers of abstraction to the abstract idea of claim 1 and therefore under prongs one and two of step 2A are also found to be ineligible.

The analysis proceeds to step 2B of the 2019 Revised Patent Subject Matter Eligibility Guidance. The structural elements in the claim are limited to what is described as a "transfer mechanism", three memories and two network interfaces along with recitations of first and second clients in the preamble. The claim also recites the capability of encryption by taking a private key and computing a cryptographic signature. In reviewing the written disclosure at paragraphs 52-53, 106 and 113 the memory and network interface are described in a manner that includes no technological improvement to the functioning of the memory and network interface and only describes a particular technological environment for which an intermediary described in paragraph 113 as a "facilitator" is linked. With regard to the encryption capabilities no particular algorithm for computing a signature is described in the written disclosure beyond the recitations at pages 17, 18 and 28 that in order to consummate a transaction that a plurality of signatures are required and the function is described at a generally high level by the written disclosure such that in the broadest reasonable interpretation the claim scope encompasses encryption that could be performed by human beings. Even if a computer calculation of the signature were inferred from the claim the written disclosure relies on prior art signature calculation mechanisms such as multisignature transactions

(see footnote 2 of page 4 of the written disclosure) or P2SH (97 and 104 of the written disclosure) and therefore do not constitute any technological improvement to the functioning of the computer itself. With regard to the two clients paragraph 110 in describing the client also describes a generic computing device with no technological improvement. The transfer mechanism per paragraphs 53, 54 and 96 are not elements of physical structure but instead are protocols involving at least decentralized currency ("Where a decentralized digital currency [e.g., the Bitcoin protocol, the Ethereum protocol, or similar] *is used as the transfer mechanism*...", 96) but per paragraph 49 can also involve centralized currency and the broadest reasonable interpretation of the term transfer mechanism can be viewed as any form of monetary exchange scheme. No technological improvement is recited in the claim nor does the combination of memories, network interfaces, transfer mechanism and two clients serve to form an ordered combination of elements that results in any technological improvement. It is abundantly clear that the claim does not involve any ordered combination of elements as the recited transfer mechanism along with the two clients do not utilize any special properties of a network or distributed computing in order to gain any technological improvement and merely are directed towards a centralized, "one-size-fits-all" technological implementation and the clients merely serve as representatives of human counterparts engaging in a contract (*BASCOM Glob. Internet Servs. v. AT&T Mobility, LLC*, 119 USPQ2d 1236 (Fed. Cir. 2016)). It is also clear that no similarity is present with regard to *McRO* (*McRO, Inc. v. Bandai Namco Games Am. Inc.*, 120 USPQ2d 1091 (Fed. Cir. 2016)) as the process applied in McRO which involved the evaluation of a plurality of subsequences of phonemes in order to set morph weights and was a

process that was not previously used by human beings in performing lip synchronization between the animated characters and the reproduced sounds. While *McRO* acknowledged that human beings could perform the operations recited in the steps it was also clear that human beings had never previously acted in such a manner, particularly as it applied to the evaluation of subsequences of phonemes in order to set the morph weights. However in the instant claims the recited operations of transferring payments and utilizing trusted intermediaries in making a payment as part of a contractual relationship are all operations that have previously been done by human beings in the same manner being claimed. It is also clear that there is no similarity to *DDR Holdings* (*DDR Holdings, LLC v. Hotels.com, LP*, 113 USPQ2d 1097 (Fed. Cir. 2014)) as there is nothing in the claims themselves or even in the written description to explicitly state or even implicitly suggest that the claims involve anything more than generic computer operations. It is also clear that there is no similarity to *Enfish* (*Enfish, LLC v. Microsoft Corp.*, 118 USPQ2d 1684 (Fed. Cir. 2016)) because nothing within the claim or the four corners of the written description provides any teaching or suggestion of an improved computer algorithm for analyzing data such as the self-referential table of *Enfish* that brings about an improvement to the computer itself where *Enfish* taught that the claimed invention brought about "increased flexibility, faster search times, and smaller memory requirements" (*Enfish* at 1690). There is also no technological improvement being made to any external technology (*Diamond v. Diehr*, 450 U.S. 175, 184 (1981)). The written disclosure at paragraphs 52-53, 106, 110 and 113 describe only the use of a generic unimproved computing environment and describes the elements in a manner that indicates that the additional elements are sufficiently well-

known that the specification does not need to describe the particulars of such additional elements to satisfy 35 U.S.C. §112 (a) and the disclosure itself recites at paragraph 108 that "The invention pertains to agreements among distinct parties that contemplate transfer of title to property, as well as any industry where that may be of value or importance" and clearly falls within the grouping of commercial/legal interactions under the groupings. ("In other words, the claims in *Diehr* were patent eligible because they improved an existing technological process, not because they were implemented on a computer", *Alice* at 1983). Therefore it is clear that no inventive concept is present sufficient to confer eligibility in light of the fact that the claims are clearly directed towards an abstract idea. Therefore claims 24, 26 and 28-29 are rejected under 35 U.S.C. § 101 as being directed towards ineligible subject matter.

Claim Rejections - 35 USC § 112

13. 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.

14. Claims 12, 15-17, 23 and 32 are 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 applications subject to pre-AIA 35 U.S.C. 112, the applicant), regards as the invention.

15. Claim 12 recites "...the transfer mechanism comprising *the decentralized digital currency* that is accessible via a computer network by the computing device..." The term "decentralized currency" lacks antecedent basis.

16. Claims 15-17 and 23 are also rejected as being dependent upon claim 12.

17. Claim 32 recites "...where the first client device and the second client device *do not trust each other*, and the computer device *is not fully trusted* by the first client device or the second client device". The term "trust" as used in the claim is a relative term

Claim Rejections - 35 USC § 103

18. 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.

19. Claims 1, 3-6, 9, 12, 15-17, 20, 23-24, 26, 28, 29 and 31-32 are rejected under 35 U.S.C. 103 as being unpatentable over Rosen (U.S. Patent Publication 2003/0070080) in view of Feigelson (U.S. Patent Publication 2013/0166455) in view of Ginter et al. (U.S. Patent Publication 2009/0030768, now U.S. Patent 7,587,369, hereinafter referred to as Ginter).

20. As per claim 1

Rosen discloses a device for processing a transaction between a first client device and a second client device via a transfer mechanism (0026, 0149-0151, 0161 "The Pay/Exchange application 35 supervises the sending and receiving of electronic notes 11 between Transaction money modules 4", Figure 56)

Rosen discloses a first memory for storing a first asymmetric key pair, the first asymmetric key pair comprising a first private key and a first public key (0162 "The Tran Log Mgr. application 36 provides the management and overseeing of a log that records completed transactions undertaken by the money module", 0189-0190, 0685-0688 "Each primary trusted server 210 has its own public key and corresponding private key", claim 1, claim 2, claim 13)

Rosen discloses a first network interface for receiving terms (0231-0234)

Rosen discloses the terms comprising at least one of a first principal data or a second principal data (0165)

Rosen discloses a reference to at least one of a first data source or a second data source (0159, 1297)

Rosen discloses an expiration timestamp (Figure 51 in element 1027, 0118, 0261, 0274, 0281) (Examiner notes that the term "expiration timestamp" appears to only be limited to a time at which something expires as a timestamp in typical usage reflects current time, not a past or future time)

Rosen discloses a computer processor coupled to the memory and the network interface, the first computer processor configured to:

read the first private key from the first key pair sector (0504, claim 13)

Rosen discloses compute a first cryptographic signature from the first private key (0660, 0662, 0702)

Rosen discloses create an inchoate data record comprising: a commit input for receiving a commit data from a commit transaction (0157, 0546, 1941)

Rosen discloses one or more output data obtained from at least one of the first principal data or the second principal data, and a value data from at least one of the first data source or the second data source (0157-0174, 0176-0179, 0184, 0535, 0798-0802)

Rosen discloses the first cryptographic signature (1946)

Rosen discloses publish the inchoate data record to at least one of the first client device and the second client device (0142-0143, 0588-0591, Figure 3, Figure 7, Figure 36A)

Rosen discloses wherein the inchoate data record is used by at least one of the first client device or the second client device to create a complete data record and to create a transaction by submitting the complete data record to the transfer mechanism (0191 “This application provides each money module with the ability to check the digital signature for authenticity. A money module receiving the digitally signed electronic note 11 can in turn sign and transfer it to others, who could also check, sign and distribute it”)

Rosen, while disclosing electronic money (Abstract), does not explicitly disclose wherein the transfer mechanism comprises a decentralized currency. Feigelson teaches wherein the transfer mechanism comprises a decentralized currency (0050-0051).

Feigelson teaches wherein the transfer mechanism comprises the decentralized digital currency that is accessible via a computer network by the computing device, the first client device, and the second client device, respectively, and the complete data record is broadcast, via the transfer mechanism to the computing device, the first client device, and the second client device for verifying and effecting the transaction (0035 “As

shown in FIG. 3, in some implementations, a digital currency network 300 (or other online value exchange system or other digital domain) may utilize a public key cryptography scheme as an addressing system. In such a scenario, a user 302 of the network (we use the term "user" broadly to include, for example, a person and any software or services used by or operated on behalf of the person, among others) will receive a public key and private key cryptographic key pair 304 either by generating such a key pair in accordance with a protocol of the digital currency network or by receiving one from another node on the network", 0037 "In some implementations, the digital currency network may be a peer-to-peer network of the kind proposed in a white paper published May 24, 2009, under the name Satoshi Nakamoto, commonly known as "Bitcoin". This network utilizes a private key and public key cryptography scheme as an addressing system")

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the electronic monetary system of Rosen with the creation and use of digital currency of Feigelson for the purpose of maintaining secrecy of information in order to control its value (0003).

Neither Rosen nor Feigelson explicitly disclose wherein an external state is observed by each of the computing device, the first client device, and the second client device and the transaction is effected when an action by at least two of the computing device, the first client device, or the second client device is detected based on the observed external state. Ginter teaches wherein an external state is observed by each of the computing device, the first client device, and the second client device and the transaction is effected when an action by at least two of the computing device, the first

client device, or the second client device is detected based on the observed external state (0312 “System 4050 can electronically pass contract 4068 along a "chain" from one party 4070 to the next ("Round Robin"), collecting signatures as it travels along. System 4050 can also allow each party 4070A-4070F to communicate with any other party. One copy of contract 4068 could be passed along from party to party and iteratively signed at the respective signers' locations. The last signer could then broadcast final, signed copies of contract 4068 to all parties. The electronic containers 302 can specify who the next recipient of contract is--forming a trusted chain of handling and control for contract 4068”, 0321 “In one example, trusted electronic go-between 4700 can also act as a mediator to resolve disputes between the contracting parties 4070A, 4070B, and can help negotiate the contract. At the conclusion of the contracting process, trusted electronic go-between 4700 may affix its own seal 4200A to the executed contract document 4068. This seal 4200A may provide a guarantee or assurance that all of the steps required by trusted electronic go-between 4700 were fulfilled before the contract 4068 was executed and that the contracting parties 4070A, 4070B are who they say they are and had authorization to execute the contract”, see also 0659-0666 “Example Contract Execution Process).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the electronic monetary system of Rosen with the creation and use of digital currency of Feigelson with the trusted and secure techniques for item delivery and execution of Ginter for the purpose of providing reliable, trusted, verifiable delivery, handling, creation and/or execution of digital items such as documents, executable code

(e.g., Java applets), and/or any other information capable of being represented in digital form (0002).

21. As per claim 3

Rosen discloses where: the computer processor is further configured to obtain the one or more output data based on: the first principal data; and the value data from the first data source (0157-0174)

22. As per claim 4

Rosen discloses where the computer processor is further configured to: compute a second cryptographic signature from the first private key; create an inchoate data record comprising: a commit input for receiving the commit data from the commit transaction: a refund output comprising a refund data; the second cryptographic signature; and a lock time; and publish the another inchoate data record to at least one of the first client device or the second client device (0157-0174, 0176-0179, 0251, 0300, 0806-0807, 0845)

23. As per claim 5

Rosen discloses where: the memory further stores a second asymmetric key pair, the second asymmetric key pair comprising a second private key and a second public key; and the computer processor is further configured to: read the second private key from the memory; compute a third cryptographic signature from the second private key; create a commit transaction data record, the commit transaction data record comprising: a first principal input for receiving the first principal data from a first principal transaction; a commit output comprising the commit data; the third cryptographic signature; and create the commit transaction by submitting the commit transaction data

record to the transfer mechanism (0177, 0193, 0546, 0662, 0791-0802, claims 1, 2 and 13)

24. As per claim 6

Rosen discloses where the first asymmetric key pair consists of the second asymmetric key pair, the first private key consists of the second private key, and the first public key consists of the second public key (0193, 0683-0688, 0854, Figure 56, claim 13)

25. As per claim 9

Rosen discloses where: the reference to the first data source comprises at least one of a reference to a base instrument and a reference to a quote instrument; and the computer processor is further configured to compute the output data on or after the expiration timestamp (0118, 0180, 0278, 0284, 0535-0540, 0628)

26. As per claim 12

Rosen discloses a device for processing a transaction between a first client device and a second client device via a transfer mechanism (0026, 0149-0151, 0161 "The Pay/Exchange application 35 supervises the sending and receiving of electronic notes 11 between Transaction money modules 4", Figure 56)

Rosen discloses a first memory comprising for storing a first asymmetric key pair, the first asymmetric key pair comprising a first private key and a first public key (0162 "The Tran Log Mgr. application 36 provides the management and overseeing of a log that records completed transactions undertaken by the money module", 0189-0190, 0685-0688 "Each primary trusted server 210 has its own public key and corresponding private key", claim 1, claim 2, claim 13)

Rosen discloses a first network interface for receiving terms (0231-0234)

Rosen discloses the terms comprising at least one of a first principal data or a second principal data (0165)

Rosen discloses a reference at least one of a first data source or a second data source (0159, 1297)

Rosen discloses an expiration timestamp (Figure 51 in element 1027, 0118, 0261, 0274, 0281) (Examiner notes that the term “expiration timestamp” appears to only be limited to a time at which something expires as a timestamp in typical usage reflects current time, not a past or future time)

Rosen discloses a first computer processor coupled to the first memory and the first network interface, the first computer processor configured to: read the first private key from the first memory (0504, claim 13)

Rosen discloses compute a first cryptographic signature from the first private key (0660, 0662, 0702)

Rosen discloses create an inchoate data record comprising: a commit input for receiving a commit data from a commit transaction (0157, 0546, 1941)

Rosen discloses one or more outputs obtained from at least one of the first principal data of the second principal data, and a value data from at least one of the first data source or the second data source (0157-0174, 0176-0179, 0184, 0535, 0798-0802)

Rosen discloses the first cryptographic signature (1946)

Rosen discloses publish the inchoate disbursement transaction record to at least one of the first client device and the second client device (0142-0143, 0588-0591, Figure 3, Figure 7, Figure 36A)

Rosen discloses where the first client device comprises: a second memory for storing a second asymmetric key pair, the second asymmetric key pair comprising a second private key and a second public key (0142-0143, 0159, 0191, 0662, 0749, claim 91)

Rosen discloses a second network interface (0666)

Rosen discloses a second computer processor coupled to the second memory and the second network interface, the second computer processor configured to read the second private key from the second memory (0630, 0664, 0749, Figure 52)

Rosen discloses read the inchoate data record; compute a second cryptographic signature from the second private key; create a complete data record comprising: the commit input; the output data; the first cryptographic signature; and the second cryptographic signature; and create a transaction by submitting the complete data record to the transfer mechanism (0157-0174, 0176-0179, 0288, 0504, 0535, 0546, 0791-0802)

Rosen discloses where the second client device comprises a third memory for storing a third asymmetric key pair, the third asymmetric key pair comprising a third private key and a third public key (1660-1663, Figure 57A)

Rosen discloses a third network interface (0670)

Rosen discloses a third computer processor coupled to the third memory and the third network interface, the third computer processor configured to read the third private key from the third key pair sector (0664, 1660-1663, Figure 56)

Rosen, while disclosing electronic money (Abstract), does not explicitly disclose wherein the transfer mechanism comprises a decentralized currency. Feigelson teaches wherein the transfer mechanism comprises a decentralized currency (0050-0051)

Feigelson teaches wherein the transfer mechanism comprises the decentralized digital currency that is accessible via a computer network by the computing device, the first client device, and the second client device, respectively, and the complete data record is broadcast, via the transfer mechanism to the computing device, the first client device, and the second client device for verifying and effecting the transaction (0035 “As shown in FIG. 3, in some implementations, a digital currency network 300 (or other online value exchange system or other digital domain) may utilize a public key cryptography scheme as an addressing system. In such a scenario, a user 302 of the network (we use the term "user" broadly to include, for example, a person and any software or services used by or operated on behalf of the person, among others) will receive a public key and private key cryptographic key pair 304 either by generating such a key pair in accordance with a protocol of the digital currency network or by receiving one from another node on the network”, 0037 “In some implementations, the digital currency network may be a peer-to-peer network of the kind proposed in a white paper published May 24, 2009, under the name Satoshi Nakamoto, commonly known

as "Bitcoin". This network utilizes a private key and public key cryptography scheme as an addressing system")

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the electronic monetary system of Rosen with the creation and use of digital currency of Feigelson for the purpose of maintaining secrecy of information in order to control its value (0003).

Neither Rosen nor Feigelson explicitly disclose wherein an external state is observed by each of the computing device, the first client device, and the second client device and the transaction is effected when an action by at least two of the computing device, the first client device, or the second client device is detected based on the observed external state. Ginter teaches wherein an external state is observed by each of the computing device, the first client device, and the second client device and the transaction is effected when an action by at least two of the computing device, the first client device, or the second client device is detected based on the observed external state (0312 "System 4050 can electronically pass contract 4068 along a "chain" from one party 4070 to the next ("Round Robin"), collecting signatures as it travels along. System 4050 can also allow each party 4070A-4070F to communicate with any other party. One copy of contract 4068 could be passed along from party to party and iteratively signed at the respective signers' locations. The last signer could then broadcast final, signed copies of contract 4068 to all parties. The electronic containers 302 can specify who the next recipient of contract is--forming a trusted chain of handling and control for contract 4068", 0321 "In one example, trusted electronic go-between 4700 can also act as a mediator to resolve disputes between the contracting parties

4070A, 4070B, and can help negotiate the contract. At the conclusion of the contracting process, trusted electronic go-between 4700 may affix its own seal 4200A to the executed contract document 4068. This seal 4200A may provide a guarantee or assurance that all of the steps required by trusted electronic go-between 4700 were fulfilled before the contract 4068 was executed and that the contracting parties 4070A, 4070B are who they say they are and had authorization to execute the contract", see also 0659-0666 "Example Contract Execution Process).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the electronic monetary system of Rosen with the creation and use of digital currency of Feigelson with the trusted and secure techniques for item delivery and execution of Ginter for the purpose of providing reliable, trusted, verifiable delivery, handling, creation and/or execution of digital items such as documents, executable code (e.g., Java applets), and/or any other information capable of being represented in digital form (0002).

27. As per claim 15

Rosen discloses where the first computer processor is further configured to: compute a third cryptographic signature from the first private key; create another inchoate data record comprising: a commit input for receiving the commit data from the commit transaction; a refund output comprising a refund data; and the third cryptographic signature; and publish the another inchoate data record to at least one of the first client and the second client. (0176-0179, 0251, 0300, 0806-0807)

28. As per claim 16

Rosen discloses where: the memory further stores a fourth asymmetric key pair, the fourth asymmetric key pair comprising a fourth private key and a fourth public key; the first computer processor is further configured to: obtain the one or more output data based on: the first principal data; and the value data from the first data source; read the fourth private key from the first memory; compute a third cryptographic signature from the fourth private key; create a commit transaction data record comprising: a first principal input for receiving the first principal data from a first principal transaction; a commit output comprising the commit data; and the third cryptographic signature; and create the commit transaction by submitting the commit transaction data record to the transfer mechanism (0157-0174, 0177, 0193, 0546, 0662, 0791-0802, claims 1, 2 and 13)

29. As per claim 17

Rosen discloses where the second computer processor is configured to: compute a fourth cryptographic signature from the second private key; create a first principal transaction data record comprising: a first principal output comprising the first principal data; and the fourth cryptographic signature; and create the first principal transaction by submitting the first principal transaction data record to the transfer mechanism (0157-0174, 0176-0179, 0300, 0791-0802)

30. As per claim 20

Rosen discloses where: the reference to at least one of the first data source or the second data source comprises at least one of a reference to a base instrument or a reference to a quote instrument; and the first computer processor is further configured

to obtain the output data on or after the expiration timestamp (0118, 0180, 0278, 0284, 0535-0540, 0628)

31. As per claim 23

Rosen discloses where: the second computer processor is further configured to: compute a third cryptographic signature from the second private key; create a first principal transaction data record comprising: a first principal output comprising the first principal data; and the third cryptographic signature; and create a first principal transaction by submitting the first principal transaction data record to the transfer mechanism; and the third computer processor is further configured to: compute a fourth cryptographic signature from the third private key; create a second principal transaction record comprising: a second principal output comprising the second principal data; and the fourth cryptographic signature; and create a second principal transaction by submitting the second principal transaction data record to the transfer mechanism (0157-0174, 0176-0179, 0300, 0490, 0662, 0791-0802)

32. As per claim 24

Rosen discloses a method for processing a transaction between a first client device and a second client device via a transfer mechanism that is accessible via a computer network by a computer device, the first client device, and the second client device (Abstract, 0149-0151, 0161, Figure 56)

Rosen discloses the transfer mechanism comprising a digital currency (0118)

Rosen discloses the method comprising: storing a first asymmetric key pair in a first memory, the first asymmetric key pair comprising a first private key and a first public key (0162, 0189-0190, 0685-688, claims 1, 2 and 13)

Rosen discloses storing a second asymmetric key pair in a second memory, the second asymmetric key pair comprising a second private key and a second public key (0142-0143, 0159, 0749, claim 91)

Rosen discloses storing a third asymmetric key pair in the second memory, the third key pair comprising a third private key and a third public key (1660-1663, Figure 57A)

Rosen discloses storing a fourth asymmetric key pair in a third memory, the fourth asymmetric key pair comprising a fourth private key and a fourth public key (0193, 0683-0688, 0854, Figure 56, claim 13)

Rosen discloses transmitting terms from one of the first or second client device via a first network interface (0231-0234) the terms comprising: at least one of a first principal data or a second principal data (0165) and a reference to at least one of a first data source or a second data source (0159, 1297) and an expiration timestamp (Figure 51 in element 1027, 0118, 0261, 0274, 0281) (Examiner notes that the term “expiration timestamp” appears to only be limited to a time at which something expires as a timestamp in typical usage reflects current time, not a past or future time)

Rosen discloses receiving the terms at the computer device via a second network interface (0026, 0589, 0666)

Rosen discloses reading the first private key from the first memory (0504, claim 13)

Rosen discloses computing a first cryptographic signature from the first private key (0660, 0662, 0702)

Rosen discloses creating a first principal transaction data record comprising: a first principal output comprising the first principal data; and the first cryptographic signature (0157-0174)

Rosen discloses creating a first principal transaction by submitting the first principal transaction data record to the transfer mechanism (0546, 0791-0802)

Rosen discloses reading the second private key from the second memory (0630, 0664, 0749, Figure 52)

Rosen discloses computing a second cryptographic signature from the second private key (0660, 0662)

Rosen discloses creating a commit transaction data record comprising: a first principal input for receiving the first principal data from the first principal transaction; a commit output comprising a commit data; and the second cryptographic signature (0157-0174, 0176-0179, 0300, 0535, 0791-0802)

Rosen discloses creating the commit transaction by submitting the commit transaction data record to the transfer mechanism (0157-0174, 0176-0179, 0300, 0535, 0791-0802)

Rosen discloses retrieving a value data from the first data source (0149, 0677)

Rosen discloses reading the third private key from the second memory (0664, 1660-1663, Figure 56)

Rosen discloses computing a third cryptographic signature from the second private key (0157-0174, 0176-0179, 0193, 0300, 0791-0802)

Rosen discloses creating an inchoate data record comprising: a commit input for receiving a commit data from the commit transaction (0157-0174, 0176-0179, 0193, 0300, 0791-0802)

Rosen discloses one or more output data obtained from the at least one of the first principal data or the second principal data and the value from the first data source (0157-0174, 0176-0179, 0184, 0535, 0798-0802)

Rosen discloses the third cryptographic signature (0157-0174, 0176-0179, 0193, 0300, 0791-0802)

Rosen discloses publishing the inchoate data record (0157-0174, 0176-0179, 0193, 0300, 0791-0802)

Rosen discloses reading the inchoate data record (0157-0174, 0176-0179, 0193, 0300, 0660, 0662, 0791-0802)

Rosen discloses reading the fourth private key from the third memory (0157-0174, 0176-0179, 0193, 0300, 0660, 0662, 0791-0802)

Rosen discloses computing a fourth cryptographic signature from the fourth private key (0157-0174, 0176-0179, 0193, 0300, 0660, 0662, 0791-0802)

Rosen discloses creating a complete data record comprising: the commit input; the one or more output data; the third cryptographic signature; and the fourth cryptographic signature (0157-0174, 0176-0179, 0193, 0300, 0660, 0662, 0791-0802)

Rosen discloses creating a transaction by submitting the complete data record to the transfer mechanism (0157-0174, 0176-0179, 0193, 0300, 0660, 0662, 0791-0802)

Rosen, while disclosing electronic money (Abstract), does not explicitly disclose wherein the transfer mechanism comprises a decentralized currency. Feigelson

teaches wherein the transfer mechanism comprises a decentralized currency (0050-0051)

Feigelson teaches broadcasting, via the transfer mechanism comprising the decentralized digital currency, the complete transaction record to the computing device, the first client device, and the second client device for verifying and effecting the transaction (0035, 0037)

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the electronic monetary system of Rosen with the creation and use of digital currency of Feigelson for the purpose of maintaining secrecy of information in order to control its value (0003).

Neither Rosen nor Feigelson explicitly disclose observing an external state. Ginter teaches observing an external state (0312 “System 4050 can electronically pass contract 4068 along a "chain" from one party 4070 to the next ("Round Robin"), collecting signatures as it travels along. System 4050 can also allow each party 4070A-4070F to communicate with any other party. One copy of contract 4068 could be passed along from party to party and iteratively signed at the respective signers' locations. The last signer could then broadcast final, signed copies of contract 4068 to all parties. The electronic containers 302 can specify who the next recipient of contract is--forming a trusted chain of handling and control for contract 4068”, 0321 “In one example, trusted electronic go-between 4700 can also act as a mediator to resolve disputes between the contracting parties 4070A, 4070B, and can help negotiate the contract. At the conclusion of the contracting process, trusted electronic go-between 4700 may affix its own seal 4200A to the executed contract document 4068. This seal

4200A may provide a guarantee or assurance that all of the steps required by trusted electronic go-between 4700 were fulfilled before the contract 4068 was executed and that the contracting parties 4070A, 4070B are who they say they are and had authorization to execute the contract", see also 0659-0666 "Example Contract Execution Process).

Ginter teaches effecting the transaction when an action by at least two of the computing device, the first client device, or the second client device is detected based on the observed external state (0312 "System 4050 can electronically pass contract 4068 along a "chain" from one party 4070 to the next ("Round Robin"), collecting signatures as it travels along. System 4050 can also allow each party 4070A-4070F to communicate with any other party. One copy of contract 4068 could be passed along from party to party and iteratively signed at the respective signers' locations. The last signer could then broadcast final, signed copies of contract 4068 to all parties. The electronic containers 302 can specify who the next recipient of contract is--forming a trusted chain of handling and control for contract 4068", 0321 "In one example, trusted electronic go-between 4700 can also act as a mediator to resolve disputes between the contracting parties 4070A, 4070B, and can help negotiate the contract. At the conclusion of the contracting process, trusted electronic go-between 4700 may affix its own seal 4200A to the executed contract document 4068. This seal 4200A may provide a guarantee or assurance that all of the steps required by trusted electronic go-between 4700 were fulfilled before the contract 4068 was executed and that the contracting parties 4070A, 4070B are who they say they are and had

authorization to execute the contract", see also 0659-0666 "Example Contract Execution Process).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the electronic monetary system of Rosen with the creation and use of digital currency of Feigelson with the trusted and secure techniques for item delivery and execution of Ginter for the purpose of providing reliable, trusted, verifiable delivery, handling, creation and/or execution of digital items such as documents, executable code (e.g., Java applets), and/or any other information capable of being represented in digital form (0002).

33. As per claim 26

Rosen discloses computing a fifth cryptographic signature from the third private key; creating another inchoate refund transaction record comprising: a commit input for receiving the commit data from the commit transaction; a refund output comprising a refund data; the fifth cryptographic signature; and a lock time; and publishing the another inchoate data record (0157-0174, 0176-0179, 0251, 0300, 0660, 0662, 0806-0807, 0845)

34. As per claim 28

Rosen discloses storing a fifth asymmetric key pair in a fourth memory, the fifth asymmetric key pair comprising a fifth private key and a fifth public key; reading the fifth private key from the fourth memory; computing a fifth cryptographic signature from the fifth private key; creating a second principal transaction data record comprising: a second principal output comprising the second principal data; and the fifth cryptographic signature; creating a second principal transaction by submitting the second principal

transaction data record to the transfer mechanism; computing one or more output data by applying a disbursement function to: the value data from the first data source; and at least one of: the first principal data; and the second principal data (0157-0174, 0176-0179, 0288, 0504, 0535, 0546, 0791-0802)

35. As per claim 29

Rosen discloses computing a sixth cryptographic signature from the third private key; creating another inchoate data record comprising: a commit input for receiving the commit data from the commit transaction; one or more refund outputs comprising one or more refund data; the sixth cryptographic signature; and a lock time; and publishing the another inchoate refund transaction data record (0157-0174, 0176-0179, 0251, 0300, 0660, 0662, 0806-0807, 0845)

36. As per claim 31

Rosen discloses wherein the one or more output data further comprise one or more conditions requiring approval of at least one of the first client device or the second client device, and the one or more conditions include a condition to determine if a sum of the one or more output data is equal or less than the commit data from the commit transaction (Figure 30 element 704, Figure 30A element 718, Figure 36 element 822, 0045, 0531-0532, 0589-0591, 1022)

37. As per claim 32

Rosen, while disclosing the presence of trusted and untrusted entities (0673, 0718) does not explicitly disclose where the first client device and the second client device do not trust each other, and the computer device is not fully trusted by the first client device or the second client device. However as no actual method step is being

claimed the language is not entitled to patentable weight per MPEP § 2103 (I)(C). Furthermore as no claim relies on whether the entities do or do not trust each the recitation is simply directed towards non-functional descriptive material that is not entitled to patentable weight per MPEP § 2111.05 (I)(A) and (B).

Conclusion

38. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

39. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JAMES D NIGH whose telephone number is (571)270-5486. The examiner can normally be reached on 5 to 7:15 AM and 10:45 AM to 4:30 PM.

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, Neha Patel can be reached on (571) 270-1492. 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.

/JAMES D NIGH/
Senior Examiner, Art Unit 3685

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/309,612	Middleton et al.
	Examiner	Art Unit
	JAMES D NIGH	3685

CPC - Searched*		
Symbol	**Date**	**Examiner**
H04L 9/3247	01/22/2021	JDN
G06Q 20/02,065,10	01/22/2021	JDN
G06Q 40/02	01/22/2021	JDN
H04L 29/06	01/22/2021	JDN
H04L 2209/38,56	01/22/2021	JDN

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**
EAST Text Search	07/18/2019	JDN
EAST Text Search	06/05/2020	JDN
PE2E Text and Classification Search	01/22/2021	JDN

	/JAMES D NIGH/ Senior Examiner, Art Unit 3685

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/309,612	Middleton et al.
	Examiner	Art Unit
	JAMES D NIGH	3685

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

	/JAMES D NIGH/ Senior Examiner, Art Unit 3685

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L1	5	("20030070080"|"20130054471"|"20130166455"|"20130179337"|"20130212388").PN.	US-PGPUB; USPAT	AND	ON	ON	2019/07/18 07:53 AM
L2	17	(server near20 ("public key") near20 ("private key")) ((transaction or principal) near10 amount) (signature near20 "private key") ((client or agent) near20 "private key") ((digital or electronic) near10 currency) @ad<="20140509"	US-PGPUB; USPAT	AND	ON	ON	2019/07/18 08:22 AM
L3	2	("20170187535").PN.	US-PGPUB; USPAT; USOCR; DERWENT	AND	ON	ON	2019/12/09 12:05 PM
L4	17	((intermediary OR server) near20 ("public key") near20 ("private key")) ((transaction or principal) near10 amount) (signature near20 "private key") ((client or agent) near20 "private key") ((digital or electronic) near10 currency) @ad<="20140509"	US-PGPUB; USPAT	AND	ON	ON	2020/06/01 12:40 PM
L5	17	((intermediary OR server) near20 ("public key") near20 ("private key")) ((transaction or principal) near10 amount) (signature near20 "private key") ((client or agent) near20 "private key") ((digital or electronic) near10 currency) (@ad<="20140509" OR @pd<="20140509" @rlad<="20140509" OR @prad<="20140509") NOT ("continuation-in-part" AND @ad>"20140509")	US-PGPUB; USPAT	AND	ON	ON	2020/06/01 12:41 PM
L6	2	((US-20130166455-A1	US-PGPUB; USPAT;	AND	ON	ON	2020/09/15

		OR US-20030070080-A1).did. AND PGPB.dbnm.)	USOCR; FIT (CN, FR, WO, JP, EP, KR); FPRS; EPO; JPO; DERWENT; IBM_TDB				12:31 PM
L7	69006	(@ad<=20140509 OR @pd<=20140509 OR @rlad<=20140509 OR @prad<=20140509) NOT ("continuation-in-part" AND @ad>20140509) oracle	US-PGPUB; USPAT	AND	ON	ON	2021/01/19 11:51 AM
L8	5	(@ad<=20140509 OR @pd<=20140509 OR @rlad<=20140509 OR @prad<=20140509) NOT ("continuation-in-part" AND @ad>20140509) (oracle near20 transaction near20 event)	US-PGPUB; USPAT	AND	ON	ON	2021/01/19 11:52 AM
L9	123593	(@ad<=20140509 OR @pd<=20140509 OR @rlad<=20140509 OR @prad<=20140509) NOT ("continuation-in-part" AND @ad>20140509) (external near5 (state OR event))	US-PGPUB; USPAT	AND	ON	ON	2021/01/19 11:53 AM
L10	158	(@ad<=20140509 OR @pd<=20140509 OR @rlad<=20140509 OR @prad<=20140509) NOT ("continuation-in-part" AND @ad>20140509) (external near5 (state OR event)) (asset near5 transaction)	US-PGPUB; USPAT	AND	ON	ON	2021/01/19 11:54 AM
L11	9104	(@ad<=20140509 OR @pd<=20140509 OR @rlad<=20140509 OR @prad<=20140509) NOT ("continuation-in-part" AND @ad>20140509) ("multi-sig" OR (multiple near3 signature))	US-PGPUB; USPAT	AND	ON	ON	2021/01/19 12:50 PM
L12	141	(@ad<=20140509 OR @pd<=20140509 OR @rlad<=20140509 OR @prad<=20140509) NOT ("continuation-in-part" AND @ad>20140509) (("multi-sig" OR (multiple	US-PGPUB; USPAT	AND	ON	ON	2021/01/19 12:50 PM

		near3 signature)) near20 transaction)					
L13	263	(@ad<=20140509 OR @pd<=20140509 OR @rlad<=20140509 OR @prad<=20140509) NOT ("continuation-in-part" AND @ad>20140509) (("multi-sig" OR (multiple near3 signature)) near20 transaction)	US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	ON	2021/01/19 02:55 PM
L14	1	(@ad<=20140509 OR @pd<=20140509 OR @rlad<=20140509 OR @prad<=20140509) NOT ("continuation-in-part" AND @ad>20140509) (("multi-sig" OR (multiple near3 signature)) near20 transaction) oracle	US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	ON	2021/01/19 02:55 PM
L15	152	(@ad<=20140509 OR @pd<=20140509 OR @rlad<=20140509 OR @prad<=20140509) NOT ("continuation-in-part" AND @ad>20140509) (notariz$4 near5 transaction)	US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	ON	2021/01/20 07:24 AM
L16	76	(@ad<=20140509 OR @pd<=20140509 OR @rlad<=20140509 OR @prad<=20140509) NOT ("continuation-in-part" AND @ad>20140509) (notariz$4 near5 transaction) contract	US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	ON	2021/01/20 08:21 AM
L17	14	(@ad<=20140509 OR @pd<=20140509 OR @rlad<=20140509 OR @prad<=20140509) NOT ("continuation-in-part" AND @ad>20140509) (notariz$4 near5 transaction) contract fulfill$5	US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	ON	2021/01/20 08:21 AM
L18	7	(@ad<=20140509 OR @pd<=20140509 OR @rlad<=20140509 OR @prad<=20140509) NOT ("continuation-in-part" AND @ad>20140509)	US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT;	AND	ON	ON	2021/01/21 07:46 AM

		(notariz$4 near5 transaction) contract fulfill$5 (H04L9/3247 OR G06Q20/065 OR G06Q40/02 OR H04L29/06 OR G06Q20/02 OR G06Q20/10 OR H04L2209/38 OR H04L2209/56).cpc.	IBM_TDB				
L19	7	((US-20130166455-A1 OR US-20030070080-A1 OR US-20150287026-A1 OR US-20090025087-A1 OR US-20090030768-A1).did. AND PGPB.dbnm.) OR ((US-20100138659-A1).did. AND DWPI.dbnm.) OR ((US-7587369-B2).did. AND USPT.dbnm.)	USPAT; US-PGPUB; FPRS; USOCR; IBM_TDB; EPO; JPO; DERWENT; FIT (AU, AP, AT, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO)	AND	ON	ON	2021/01/21 07:46 AM
L21	2	(@ad<=20140509 OR @pd<=20140509 OR @rlad<=20140509 OR @prad<=20140509) NOT ("continuation-in-part" AND @ad>20140509) (notariz$4 near5 transaction) contract fulfill$5 untrusted	US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	ON	2021/01/22 10:50 AM
L22	5	(@ad<=20140509 OR @pd<=20140509 OR @rlad<=20140509 OR @prad<=20140509) NOT ("continuation-in-part" AND @ad>20140509) (notariz$4 near5 transaction) contract untrusted	US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	ON	2021/01/22 10:50 AM

PE2E SEARCH - Search History (Interference)

There are no Interference searches to show.

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
15/309,612	11/08/2016	Reginald Middleton	4675.1002BS

CONFIRMATION NO. 2321

86636
BRUNDIDGE & STANGER, P.C.
1925 BALLENGER AVENUE, STE. 560
ALEXANDRIA, VA 22314

IMPROPER CFR REQUEST

OC00000012343037 3

Date Mailed: 02/17/2021

RESPONSE TO REQUEST FOR CORRECTED FILING RECEIPT

Power of Attorney, Claims, Fees, System Limitations, and Miscellaneous

In response to your request for a corrected Filing Receipt, the Office is unable to comply with your request because:

- The ADS submitted on 01/21/2021 attempts to change the applicant but cannot be entered. Any request to change the applicant once the applicant has been specified must include (1) an application data sheet specifying the new applicant in the Applicant Information section, and (2) a statement under 37 CFR 3.73(c) (USPTO Form PTO/AIA/96 or an equivalent) to show chain of title to the new applicant. The application data sheet must contain markings to show the information that is being changed, with underlining for additions and strike-through or brackets for deletions. See 37 CFR 1.76(c)(2).

In order to make changes to the information of record, an ADS must be properly signed and properly marked up relative to the current information of record.

Proper signature: The ADS must be signed with a handwritten signature or proper S-signature by:

- A patent practitioner, with the practitioner's registration number accompanying the signature (e.g., immediately below or adjacent to the signature), or
- The applicant, if the applicant is an individual other than the inventor(s) and no power of attorney has been appointed, or
- All of the inventors, if no other applicant has been established and no power of attorney has been appointed.

A proper S-signature consists of only letters and/or Arabic numerals, with appropriate spaces and commas, periods, apostrophes, or hyphens for punctuation contained between a first single forward slash mark before, and a second single forward slash mark after, the S-signature.

Proper markings: The ADS must identify the changes being made with underlining for insertions and strike-through or brackets for text removed. No other markings or indications are acceptable. Where an ADS providing corrected or updated information does not contain all of the sections of the ADS, the entire section in which changes are being made must be included in the ADS. Information of record can generally be found on the latest filing receipt.

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**.

/fasrat/

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. 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	~~2626.P100.US~~ 4675.1002BS
	Application Number	15/309,612
Title of Invention	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers	

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
	Reginald		Middleton	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Brooklyn	State/Province	NY	Country of Residence	US

Mailing Address of Inventor:

Address 1	195 Argyle Road		
Address 2			
City	Brooklyn	State/Province	NY
Postal Code	11218	Country	US

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Matthew		Bogosian	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Anacortes	State/Province	WA	Country of Residence	US

Mailing Address of Inventor:

Address 1	5007 Totem Trl		
Address 2			
City	Anacortes	State/Province	WA
Postal Code	98221	Country	US

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).

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. 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	~~2626.P100.US~~ 4675.1002BS
	Application Number	15/309,612
Title of Invention	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers	

☐ An Address is being provided for the correspondence Information of this application.			
Customer Number	~~115238~~ 86636		
Email Address	mail@brundidge-slanger.com	Add Email	Remove Email

Application Information:

Title of the Invention	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers		
Attorney Docket Number	~~2626.P100.US~~ 4675.1002BS	**Small Entity Status Claimed** ☒	
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	16	**Suggested Figure for Publication (if any)**	1

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.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	~~115238~~ 86636		

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	~~2626.P100.US~~ 4675.1002BS
	Application Number	15/309,612
Title of Invention	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers	

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)
~~PCT/US15/29196~~ 15/309,612	a 371 of international	PCT/US15/29196	2015-05-05
Prior Application Status	~~Pending~~ Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
~~61/990795~~ PCT/US15/29196	Claims benefit of provisional	61/990,795	2014-05-09

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.

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)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button.

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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	~~2626.P100.US~~ 4675.1002BS
	Application Number	15/309,612
Title of Invention	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers	

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 (11-15)
Approved for use through 04/30/2017. 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	~~2626.P100.US~~ 4675.1002BS
	Application Number	15/309,612
Title of Invention	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers	

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

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~~	~~Veritaseum, Inc.~~ Reginald Middleton

Mailing Address Information For Applicant:

Address 1	195 Argyle Road		
Address 2			
City	Brooklyn	**State/Province**	NY
Country	US	Postal Code	11218
Phone Number	718-407-4756	Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button.

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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	~~2626.P100.US~~ 4675 1002BS
	Application Number	15/309,612
Title of Invention	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers	

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.

If the Assignee or Non-Applicant Assignee is an Organization check here. ☒

~~Organization~~ Name	Reginald Middleton

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1	195 Argyle Road		
Address 2			
City	Brooklyn	**State/Province**	NY
Country i	US	Postal Code	11218
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.

Signature:

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	~~/JohnNielsen53392/~~ /Misung Lee/			Date (YYYY-MM-DD)	~~2016-11-04~~ 2021-02-22
First Name	~~John~~ Misung	Last Name	~~Nielsen~~ Lee	Registration Number	~~53,392~~ 78,307

Additional Signature may be generated within this form by selecting the Add button.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. 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	~~2626.P100.US~~ 4675.1002BS
	Application Number	15/309,612
Title of Invention	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers	

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.**

Electronic Acknowledgement Receipt

EFS ID:	41978513
Application Number:	15309612
International Application Number:	
Confirmation Number:	2321
Title of Invention:	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers
First Named Inventor/Applicant Name:	Reginald Middleton
Customer Number:	86636
Filer:	Misung Lee/Juel Clyne
Filer Authorized By:	Misung Lee
Attorney Docket Number:	4675.1002BS
Receipt Date:	22-FEB-2021
Filing Date:	08-NOV-2016
Time Stamp:	10:15:29
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	Application Data Sheet	4675_20210222_CorrectedADS2.pdf	408095 8ef84eb7c392281938754b11a139386489fa93ad	no	7

Warnings:

Information:					
This is not an USPTO supplied ADS fillable form					
2	Miscellaneous Incoming Letter	4675_20210222_Corrected_ADS_Response.pdf	39185 ef832cc663413558db0c5606185b300a6c5d3da8	no	1
Warnings:					
Information:					
3	Assignee showing of ownership per 37 CFR 3.73	4675_373.pdf	123499 1cb32ff092c596231442cd74df61a2fb420ca04d	no	3
Warnings:					
Information:					
			Total Files Size (in bytes):	570779	

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.

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: MIDDLETON, REGINALD

Application No./Patent No.: 15309612 Filed/Issue Date: November 8, 2016

Titled: Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers

MIDDLETON, REGINALD, a individual

(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 049973, Frame 0680, 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.

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.

/Misung Lee/	2021-02-22
Signature	Date
Misung Lee	78307
Printed or Typed Name	Title or Registration Number

[Page 2 of 2]

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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application Serial No. 15/309,612
Filing Date ..... November 08, 2016
Confirmation No. 2321
Inventorship ..... Reginald Middleton
Group Art Unit 3685
Examiner ..... NIGH, JAMES D
Attorney Docket No. 4675.1002BS
Title: ..... Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers

REQUEST TO CORRECT APPLICATION DATA SHEET

To: Commissioner for Patents
Office of Initial Patent Examination
P.O. Box 1450
Alexandria, VA 22313-1450

February 22, 2021

From: Misung Lee
Customer No. 86636
Brundidge & Stanger, PC
1925 Ballenger Ave. Ste 560
Alexandria, VA 22314

Sir:

It is respectfully submitted herewith a corrected Application Date Sheet (ADS) to correctly list Applicant information as:

"~~Veritaseum, Inc.~~" to "Reginald Middleton"

A patent assignment (Reel/Frame: 049973/0680) indicating Reginald Middleton as an assignee was recorded on August 6, 2019 with the USPTO. Further, a statement under 37 CFR 3.73(c) is submitted herewith.

It is respectfully requested that a Corrected Filing Receipt be issued stating the correct Applicant information. Please charge any fees or credit any overpayment to Deposit Account No.: 50-4888.

Respectfully submitted,

/Misung Lee/
Misung Lee
Reg. No. 78,307

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
15/309,612	11/08/2016	3685	960	4675.1002BS	30	3

CONFIRMATION NO. 2321

CORRECTED FILING RECEIPT

86636
BRUNDIDGE & STANGER, P.C.
1925 BALLENGER AVENUE, STE. 560
ALEXANDRIA, VA 22314

OC000000125359490

Date Mailed: 05/04/2021

Receipt is acknowledged of this non-provisional utility 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 FIRST INVENTOR, 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 corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction 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 provided that the request is grantable.

Inventor(s)

Reginald Middleton, Brooklyn, NY;
Matthew Bogosian, Anacortes, WA;

Applicant(s)

Reginald Middleton, Brooklyn, NY;

Assignment For Published Patent Application

Reginald Middleton, Brooklyn, NY

Power of Attorney: The patent practitioners associated with Customer Number 86636

Domestic Priority data as claimed by applicant

This application is a 371 of PCT/US15/29196 05/05/2015
which claims benefit of 61/990,795 05/09/2014

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

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: 03/20/2017

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 15/309,612**

Projected Publication Date: Not Applicable

Non-Publication Request: No

Early Publication Request: No

**** SMALL ENTITY ****

Title

Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers

Preliminary Class

705

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.

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.
15/309,612	11/08/2016	Reginald Middleton	4675.1002BS	2321

86636 7590 05/10/2021

BRUNDIDGE & STANGER, P.C.
1925 BALLENGER AVENUE, STE. 560
ALEXANDRIA, VA 22314

EXAMINER	
NIGH, JAMES D	

ART UNIT	PAPER NUMBER
3685	

MAIL DATE	DELIVERY MODE
05/10/2021	PAPER

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.

Applicant-Initiated Interview Summary	Application No. 15/309,612	Applicant(s) Middleton et al.		
	Examiner JAMES D NIGH	Art Unit 3685	AIA (First Inventor to File) Status Yes	Page 1 of 2

All Participants (applicant, applicants representative, PTO personnel)	Title	Type
JAMES D NIGH	Primary Examiner	Telephonic
Misung Li (Reg. No. 78,307)	Attorney	
Carl Brundidge (Reg. No. 29,621)	Attorney	
Reginal Middleton	Inventor	
Matthew Bogosian	Inventor	

Date of Interview: 06 May 2021

Issues Discussed:

35 U.S.C. 101

Discussed what constitutes an element under the 2019 PEG under Prong Two of Step 2A and how it impacts the analysis under the 2019 PEG. No agreement was reached. Examiner agreed to send recent Board decisions to Applicant and Applicant indicated that they would include Board decisions in their response.

35 U.S.C. 103

Discussed the Rosen and Feigelson references cited in the rejection and specifically the combinability of the two references. No agreement was reached.

☑ Attachment

	/JAMES D NIGH/ Senior Examiner, Art Unit 3685

Applicant is reminded that a complete written statement as to the substance of the interview must be made of record in the application file. It is the applicants responsibility to provide the written statement, unless the interview was initiated by the Examiner and the Examiner has indicated that a written summary will be provided. See MPEP 713.04
Please further see:
MPEP 713.04
Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews, paragraph (b)
37 CFR § 1.2 Business to be transacted in writing

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete

and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

Application Serial No 15/309,612
Filing Date ..... November 08, 2016
Confirmation No 2321
Inventorship ..... Reginald Middleton
Group Art Unit 3685
Examiner ..... NIGH, JAMES D
Attorney Docket No 4675.1002BS
Title: ..... DEVICES, SYSTEMS, AND METHODS FOR FACILITATING LOW TRUST AND ZERO TRUST VALUE TRANSFERS

To: Examiner Nigh

From: Misung Lee (T. 703-718-4018)
Brundidge & Stanger, PC
1925 Ballenger Avenue, Suite 560
Alexandria, VA 22314

Examiner Nigh:

Please consider the following in anticipation of our conversation during an interview.

FOR DISCUSSION PURPOSE ONLY

35 U.S.C. § 101

Applicant's representative would like to discuss regarding proposed amendments of Claim 1 as below (emphasis added):

1. (**Currently Amended**) A computing device for processing a transaction between a first client device, and a second client device via a transfer mechanism, the transfer mechanism comprising a decentralized digital currency, the computing device comprising:

a memory for storing a first asymmetric key pair, the first asymmetric key pair comprising a first private key and a first public key;

a network interface for receiving terms, the terms comprising:

~~at least one of~~ a first principal data and a first collateral data, or a second principal data and a second collateral data;

a reference to at least one of a first data source or a second data source; and

an expiration timestamp;

a computer processor coupled to the memory and the network interface, the computer processor configured to:

read the first private key from the memory;

compute a first cryptographic signature from the first private key;

create an inchoate data record comprising:

a commit input for receiving a commit data from a commit transaction;

one or more output data obtained from ~~at least one of~~ the first principal data and the first collateral data, or the second principal data and the second collateral data, and a value data from at least one of the first data source or the second data source; and

the first cryptographic signature; and

publish the inchoate data record to at least one of the first client device or the second client device,

wherein the decentralized digital currency comprises a distributed ledger that enables processing the transaction between the first client device and the second client device without a trusted central authority,

wherein the inchoate data record is used by at least one of the first client device or the second client device to create a complete data record and to create ~~a~~ the transaction by ~~submitting~~ broadcasting the complete data record ~~to the transfer mechanism~~for transmitting and receiving among network participants in the computer network for recording in the distributed ledger,

wherein the at least one of the first client device or the second client device signs the inchoate data record and saves a copy of the inchoate data record on the at least one of the first client device or the second client device; and

~~wherein the transfer mechanism comprises the decentralized digital currency that is accessible via a computer network by the computing device, the first client device, and the second client device, respectively, and the complete data record is broadcast, via the transfer mechanism to the computing device, the first client device, and the second client device for verifying and effecting the transaction,~~ wherein the at least one of the computing device, the first client device, or the second client device verifies the recording of the complete data record in the distributed ledger by observing an external state ~~is observed by each of the computing device, the first client device, and the second client device and the transaction is effected when an action by at least two of the computing device, the first client device, or the second client device is detected based on the observed external state~~.

Currently amended Claim 1 is directed to a specific computing device for enabling increased security for either party entering into the transaction via a decentralized digital currency of the transfer mechanism, which comprises a distributed ledger, without requiring a trusted central authority. Furthermore, the computing device as recited in Claim 1 participates in the transaction, but the computing device alone cannot control disposition. Instead, the computing device only effects the transaction between the client devices in conjunction with the participation of one of the first or second client device and only in a fashion that was previously and unanimously agreed upon by both parties, and either the first and/or second client device is responsible for ultimately administering the transaction via the decentralized digital currency which comprises a distributed ledger.

The claimed decentralized digital currency prevents the computer device from being commandeered to effect transaction not contemplated by at least one of the first or second client device. As argued in the previously filed Response, the computer device is *a distributed participant* that works in connection with the first and second client device in a decentralized role (the antithesis of a centralized actor, authority or entity), ensuring not only that it is not centralized, but enabling transactions *without the inclusion or involvement of centralized, costly third-party intermediaries who traditionally may otherwise be required, and without traditional exposure to counterparty risk*. Further, as described in paragraph [0339] of the present application, "transaction" is to refer to the part of a ledger or block within a distributed ledger comprising the "transaction record" wherein the "transaction record" is a data structure describing a transaction and submitted to a transfer mechanism to effect a transaction. The claimed computer instructions which verify and execute its terms upon the occurrence of the predetermined events do not correspond to "fundamental economic practice" or "a commercial/legal interaction," as alleged by the Office Action. It is respectfully submitted that the feature of amended Claim 1 is implemented on the *decentralized digital currency, distributed ledger* that is not to be a "fundamental" economic practice or "a commercial/legal interaction."

It is further respectfully submitted that the use of the distributed ledger differs from a generic computer component that performs processes which could be performed in the mind or using pen and paper. For

example, the distributed nature of the distributed ledger requires a copy of the ledger to be stored on different nodes across the network. A person cannot do the above simply in their mind or simply using pen and paper and the claimed features associated with the distributed nature of technology do not fall into "organizing of human activity" as alleged by the Office Action.

Please also see PTAB appeal decision 2019-004127 decided August 19, 2020.

35 U.S.C. § 103

It is respectfully submitted that the proposed combination of the cited references fails to teach or suggest above recitation of Claim 1.

In primary reference Rogen, as acknowledged by the Office Action, while disclosing electronic money (Abstract), does not explicitly disclose wherein the transfer mechanism comprises a decentralized currency. The Examiner alleges that Feigelson teaches wherein the transfer mechanism comprises a decentralized currency (0050-0051), and it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the electronic monetary system of Rosen with the creation and use of digital currency of Feigelson for the purpose of maintaining secrecy of information in order to control its value (0003).

Rosen identifies intermediaries who store and control currency (value) as agents or intermediaries or promissories. For example, Rosen describes various scenarios, all of which involve such controlling intermediaries like deposit banks, correspondent banks, participating banks, issuing banks, and clearing banks, see Rosen, at paragraph [0026]. Further, Rosen describes mechanisms using cryptography managed by a central authority for the sole purpose of authentication (see Rosen, paragraph [0191]). Further still, Rosen describes trusted agents 2, 4 for both the customer and merchant (see Rosen, paragraph [0630]).

From the above descriptions, it is noted that Rosen requires (i)a trusted centralized facilitator (intermediary), (ii) a trusted agent for merchant and customer, and (iii) a certificate central authority.

Rosen and Fergerson are not combinable. The proposed combination of Rosen and Feigelson would impermissibly render Feigelson unsatisfactory for its intended purpose because all benefits derived from Feigelson are lost when moving from tokens as described by Feigelson to conventional forms of account as described by Rosen. There is no way to combine Feigelson with Rosen that retains the advantages of Feigelson's disclosure. Therefore, modifying Feigelson by adding features described in Rosen would impermissibly render Feigelson unsatisfactory for its intended purpose of providing security features for the physical devices that carry values. Moreover, the proposed modification would impermissibly change the principle of operation of Feigelson.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application Serial No..... 15/309,612
Filing Date ..... November 08, 2016
Confirmation No. 2321
Inventorship ..... Reginald Middleton
Group Art Unit..... 3685
Examiner .....NIGH, JAMES D
Attorney Docket No. 4675.1002BS
Title:.....DEVICES, SYSTEMS, AND METHODS FOR FACILITATING LOW TRUST AND ZERO TRUST VALUE TRANSFERS

RESPONSE TO FINAL OFFICE ACTION OF JANUARY 27, 2021,
STATEMENT OF SUBSTANCE OF INTERVIEW, AND
AND REQUEST FOR CONTINUED EXAMINATION UNDER 37 CFR 1.114

To: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

From: Misung Lee
Customer No. 86636
Brundidge & Stanger, PC
1925 Ballenger Ave., Suite 560
Alexandria, VA 22314

Sir:

In response to the Final Office Action dated January 27, 2021, for which the three-month shortened statutory period for response is extended to expire on July 27, 2021, and subsequent to the Examiner Interview conducted on May 6, 2021, the following amendments and remarks are respectfully submitted with the concurrently filed Request for Continued Examination in compliance with 37 CFR § 1.114. Favorable consideration is respectfully requested.

The Commissioner is hereby authorized to charge any deficiency of fees and credit any overpayments to Deposit Account Number 50-4888.

INTRODUCTORY COMMENTS

The Listing of the Claims section begins on page 3.

Remarks section begins on page 19.

LISTING OF THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Claims pending:

- At time of the Action: **Claims 1, 3-6, 9, 12, 15-17, 20, 23, 24, 26, 28, 29, 31, and 32**
- After this Reply: **Claims 1, 3-6, 9, 12, 15-17, 20, 23, 24, 26, 28, 29, 31, and 33**

Currently Canceled or Withdrawn Claims: Claim 32

Currently Amended Claims: Claims 1, 12, 24 and 28

New Claims: Claim 33

1. (**Currently Amended**) A computing device for processing a transaction between a first client device, and a second client device via a transfer mechanism, the transfer mechanism comprising a decentralized digital currency, the computing device comprising:

a memory for storing a first asymmetric key pair, the first asymmetric key pair comprising a first private key and a first public key;

a network interface for receiving terms, the terms comprising:

at least one of a first principal data or a second principal data;

a reference to at least one of a first data source or a second data source; and

an expiration timestamp;

a computer processor coupled to the memory and the network interface, the computer processor configured to:

read the first private key from the memory;

compute a first cryptographic signature from the first private key;

create an inchoate data record comprising:

a commit input for receiving a commit data from a commit transaction;

one or more output data obtained from at least one of the first principal data or the second principal data, and a value data from at least one of the first data source or the second data source; and

the first cryptographic signature; and

publish the inchoate data record to at least one of the first client device or the second client device,

wherein the decentralized digital currency comprises a distributed ledger that enables processing the transaction between the first client device and the second client device without the need for a trusted central authority,

wherein the inchoate data record is used by at least one of the first client device or the second client device to create a complete data record and to create ~~a~~ the transaction by ~~submitting~~ broadcasting the complete data record ~~to the transfer mechanism~~for transmitting and receiving among network participants in the computer network for recording in the distributed ledger,

wherein at least one of the first client device or the second client device signs the inchoate data record and saves a copy of the inchoate data record on at least one of the first client device or the second client device; and

~~wherein the transfer mechanism comprises the decentralized digital currency that is accessible via a computer network by the computing device, the first client device, and the second client device, respectively, and the complete data record is broadcast, via the transfer mechanism to the computing device, the first client device, and the second client device for verifying and effecting the transaction,~~ wherein the at least one of the computing device, the first client device, or the second client device verifies the recording of the complete data record

in the distributed ledger by observing an external state ~~is observed by each of the computing device, the first client device, and the second client device and the transaction is effected when an action by at least two of the computing device, the first client device, or the second client device is detected based on the observed external state~~.

2. (**Canceled**)

3. (**Previously Presented**) The device of claim 1, where:

the computer processor is configured to obtain the one or more output data based on:

the first principal data; and

the value data from the first data source.

4. (**Previously Presented**) The device of claim 1, where the computer processor is further configured to:

compute a second cryptographic signature from the first private key;

create an another inchoate data record comprising:

a commit input for receiving the commit data from the commit transaction;

a refund output comprising a refund data;

the second cryptographic signature; and

a lock time; and

publish the another inchoate data record to at least one of the first client device or the second client device.

5. (**Previously Presented**) The device of claim 1, where:

the memory further stores a second asymmetric key pair, the second asymmetric key pair comprising a second private key and a second public key; and

the computer processor is further configured to:

read the second private key from the memory;

compute a third cryptographic signature from the second private key;

create a commit transaction data record, the commit transaction data record comprising:

a first principal input for receiving the first principal data from a first principal transaction;

a commit output comprising the commit data;

the third cryptographic signature; and

create the commit transaction by submitting the commit transaction data record to the transfer mechanism.

6. (**Previously Presented**) The device of claim 5, where the first asymmetric key pair consists of the second asymmetric key pair, the first private key consists of the second private key, and the first public key consists of the second public key.

7. (**Canceled**)

8. (**Canceled**)

9. (**Previously Presented**) The device of claim1, where:

the reference to the first data source comprises at least one of a reference to a base instrument and a reference to a quote instrument; and

the computer processor is further configured to compute the output data on or after the expiration timestamp.

10. (**Canceled**)

11. (**Canceled**)

12. (**Currently Amended**) A system for processing a transaction between a first client device and a second client device via a transfer mechanism,[[,]] the system comprising a computing device, the first client device, the second client device, and the transfer mechanism;

the computing device comprising:

a first memory comprising for storing a first asymmetric key pair, the first asymmetric key pair comprising a first private key and a first public key;

a first network interface for receiving terms, the terms comprising:

at least one of a first principal data or a second principal data;

a reference to at least one of a first data source or a second data source; and

an expiration timestamp; and

a first computer processor coupled to the first memory and the first network interface, the first computer processor configured to:

read the first private key from the first memory;

compute a first cryptographic signature from the first private key;

create an inchoate data record comprising:

a commit input for receiving a commit data from a commit transaction;

one or more outputs obtained from at least one of the first principal data or the second principal data, and a value data from at least one of the first data source or the second data source; and

the first cryptographic signature; and

publish the inchoate data record to at least one of the first client device or the second client device;

the first client device comprising:

a second memory for storing a second asymmetric key pair, the second asymmetric key pair comprising a second private key and a second public key;

a second network interface; and

a second computer processor coupled to the second memory and the second network interface, the second computer processor configured to:

read the second private key from the second memory;

read the inchoate data record;

compute a second cryptographic signature from the second private key;

create a complete data record comprising:

the commit input;

the output data;

the first cryptographic signature; and

the second cryptographic signature; and

create a transaction by submitting the complete data record to the transfer mechanism;

the second client device comprising:

a third memory for storing a third asymmetric key pair, the third asymmetric key pair comprising a third private key and a third public key;

a third network interface; and

a third computer processor coupled to the third memory and the third network interface, the third computer processor configured to read the third private key from the third memory; and

wherein the at least one of the first client device or the second client device signs the inchoate data record and saves a copy of the inchoate data record on at least one of the first client device or the second client device,

wherein the transfer mechanism comprising ~~the~~ a decentralized digital currency that comprises a distributed ledger that ~~is accessible via a computer network by the computing device, the first client device, and the second client device, respectively, the transfer mechanism configured to~~ enables processing the transaction between the first client device and the second client device without the need for a trusted central authority,

wherein the transaction is created by broadcasting the complete data record ~~to~~ for transmitting and receiving among network participants in the computer network for recording in the distributed ledger, and

wherein at least one of the computer device, the first client device, ~~and~~ or the second client device ~~for verifying and effecting the transaction,~~ verifies the recording of the complete data record in the distributed ledger by ~~wherein~~observing an external state ~~is observed by each of the computer device, the first client device, and the second client device, and the transaction is effected when an action by at least two of the computer device, the first client device, or the second client device is detected based on the observed external state~~.

13. (**Canceled**)

14. (**Canceled**)

15. (**Previously Presented**) The system of claim 12, where the first computer processor is further configured to:

compute a third cryptographic signature from the first private key;

create another inchoate data record comprising:

a commit input for receiving the commit data from the commit transaction;

a refund output comprising a refund data; and

the third cryptographic signature; and

publish the another inchoate data record to at least one of the first client and the second client.

16. (**Previously Presented**) The system of claim 12, where:

the first memory further stores a fourth asymmetric key pair, the fourth asymmetric key pair comprising a fourth private key and a fourth public key;

the first computer processor is further configured to:

obtain the one or more output data based on:

the first principal data ; and

the value data from the first data source;

read the fourth private key from the first memory;

compute a third cryptographic signature from the fourth private key;

create a commit transaction data record comprising:

a first principal input for receiving the first principal data from a first principal transaction;

a commit output comprising the commit data; and

the third cryptographic signature; and

create the commit transaction by submitting the commit transaction data record to the transfer mechanism.

17. (**Previously Presented**) The system of claim 16, where the second computer processor is configured to:

compute a fourth cryptographic signature from the second private key;

create a first principal transaction data record comprising:

a first principal output comprising the first principal data; and

the fourth cryptographic signature; and

create the first principal transaction by submitting the first principal transaction data record to the transfer mechanism.

18. (**Canceled**)

19. (**Canceled**)

20. (**Previously Presented**) The system of claim 12, where:

the reference to at least one of the first data source or the second data source comprises at least one of a reference to a base instrument or a reference to a quote instrument; and

the first computer processor is further configured to obtain the output data on or after the expiration timestamp.

21. (**Canceled**)

22. (**Canceled**)

23. (**Previously Presented**) The system of claim 12, where:

the second computer processor is further configured to:

compute a third cryptographic signature from the second private key;

create a first principal transaction data record comprising:

a first principal output comprising the first principal data; and

the third cryptographic signature; and

create a first principal transaction by submitting the first principal transaction data record to the transfer mechanism; and

the third computer processor is further configured to:

compute a fourth cryptographic signature from the third private key;

create a second principal transaction data record comprising:

a second principal output comprising the second principal data; and

the fourth cryptographic signature; and

create a second principal transaction by submitting the second principal transaction data record to the transfer mechanism.

24. (**Currently Amended**) A method for processing a transaction between a first client device and a second client device via a transfer mechanism, the transfer mechanism comprising a decentralized digital currency comprising a distributed ledger that is accessible via a computer network by a computer device, the first client device, and the second client device, respectively, the method comprising:

storing a first asymmetric key pair in a first memory, the first asymmetric key pair comprising a first private key and a first public key;

storing a second asymmetric key pair a second memory, the second asymmetric key pair comprising a second private key and a second public key;

storing a third asymmetric key pair in the second memory, the third key pair comprising a third private key and a third public key;

storing a fourth asymmetric key pair in a third memory, the fourth asymmetric key pair comprising a fourth private key and a fourth public key;

transmitting terms from one of the first or second client device via a first network interface, the terms comprising:

at least one of a first principal data or a second principal data;

a reference to at least one of a first data source or a second data source; and

an expiration timestamp;

receiving the terms at the computer device via a second network interface;

reading the first private key from the first memory;

computing a first cryptographic signature from the first private key;

creating a first principal transaction data record comprising:

a first principal output comprising the first principal data; and

the first cryptographic signature;

creating a first principal transaction by submitting the first principal transaction data record to the transfer mechanism;

reading the second private key from the second memory;

computing a second cryptographic signature from the second private key;

creating a commit transaction data record comprising:

a first principal input for receiving the first principal data from the first principal transaction;

a commit output comprising a commit data; and

the second cryptographic signature;

creating the commit transaction by submitting the commit transaction data record to the transfer mechanism;

retrieving a value data from the first data source;

reading the third private key from the second memory;

computing a third cryptographic signature from the second private key;

creating an inchoate data record comprising:

a commit input for receiving a commit data from the commit transaction;

one or more output data obtained from ~~the~~ at least one of the first principal data or the second principal data and the value from the first data source; and

the third cryptographic signature;

publishing the inchoate data record;

reading the inchoate data record;

signing the inchoate data record and saving a copy of the inchoate data record on at least one of the first client device or the second client device;

reading the fourth private key from the third memory;

computing a fourth cryptographic signature from the fourth private key;

creating a complete data record comprising:

the commit input;

the one or more output data;

the third cryptographic signature; and

the fourth cryptographic signature;

creating ~~a~~the transaction by ~~submitting~~ broadcasting the complete data record ~~to the transfer mechanism~~ for transmitting and receiving among network participants in the computer network for recording in the distributed ledger; and

~~broadcasting, via the transfer mechanism comprising the decentralized digital currency, the complete transaction record to the computing device, the first client device, and the second client device for~~ verifying, via at least one of the computing device, the first client device, or the second client device, ~~and effecting the transaction;~~ the recording of the complete data record in the distributed ledger by observing an external state~~; and~~

~~effecting the transaction when an action by at least two of the computing device, the first client device, or the second client device is detected based on the observed external state.~~,

wherein the distributed ledger enables processing the transaction between the first client device and the second client device without the need for a trusted central authority.

25. (**Canceled**)

26. (**Previously Presented**) The method of claim24, further comprising:

computing a fifth cryptographic signature from the third private key;

creating another inchoate data record comprising:

a commit input for receiving the commit data from the commit transaction;

a refund output comprising a refund data;

the fifth cryptographic signature; and

a lock time; and

publishing the another inchoate data record.

27. (**Canceled**)

28. (**Previously Presented**) The method of claim 24, further comprising:

storing a fifth asymmetric key pair in a fourth memory, the fifth asymmetric key pair comprising a fifth private key and a fifth public key;

reading the fifth private key from the fourth memory;

computing a fifth cryptographic signature from the fifth private key;

creating a second principal transaction data record comprising:

a second principal output comprising the second principal data; and

the fifth cryptographic signature;

creating a second principal transaction by submitting the second principal transaction data record to the transfer mechanism;

computing one or more output data by applying a disbursement function to:

the value data from the first data source; and at least one of:

the first principal data; and

the second principal data.

29. (**Previously Presented**) The method of claim 28, further comprising:

computing a sixth cryptographic signature from the third private key;

creating another inchoate data record comprising:

a commit input for receiving the commit data from the commit transaction;

one or more refund outputs comprising one or more refund data;

the sixth cryptographic signature; and

a lock time; and

publishing the another inchoate data record.

30. (**Canceled**)

31. (**Previously Presented**) The method of claim 24, wherein the one or more output data further comprise one or more conditions requiring approval of at least one of the first client device or the second client device, and the one or more conditions include a condition to determine if a sum of the one or more output data is equal or less than the commit data from the commit transaction.

32. (**Canceled**)

33. (**New**) The method of claim 24, wherein the terms further comprise a first collateral data, or a second collateral data;

wherein the first principal transaction data record further comprises a first collateral output comprising the first collateral data;

wherein the commit transaction data record further comprises a first collateral input for receiving the first collateral data from the first principal transaction; and

wherein the one or more output data is obtained from the first principal data and the first collateral data or the second principal data and the second collateral data, and the value from the first data source.

Electronic Acknowledgement Receipt

EFS ID:	43357564
Application Number:	15309612
International Application Number:	
Confirmation Number:	2321
Title of Invention:	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers
First Named Inventor/Applicant Name:	Reginald Middleton
Customer Number:	86636
Filer:	Misung Lee/Juel Clyne
Filer Authorized By:	Misung Lee
Attorney Docket Number:	4675.1002BS
Receipt Date:	27-JUL-2021
Filing Date:	08-NOV-2016
Time Stamp:	21:52:44
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	$1740
RAM confirmation Number	E20217QL53084435
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	Fee Worksheet (SB06)	fee-info.pdf	40776 265963aa1c3aae1f8d057b42b2e84e8e9421f61e	no	2

Warnings:	
Information:	
Total Files Size (in bytes):	40776

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.

Electronic Acknowledgement Receipt

EFS ID:	43355243
Application Number:	15309612
International Application Number:	
Confirmation Number:	2321
Title of Invention:	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers
First Named Inventor/Applicant Name:	Reginald Middleton
Customer Number:	86636
Filer:	Misung Lee
Filer Authorized By:	
Attorney Docket Number:	4675.1002BS
Receipt Date:	27-JUL-2021
Filing Date:	08-NOV-2016
Time Stamp:	15:45:24
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	Response After Final Action	4675_20210727_FOA_Response.pdf	312757 ef5bd492893ae02c34820656cf6e28e8ca545b0b	no	46

Warnings:

Information:					
2	Request for Continued Examination (RCE)	4675_20210727_RCE.pdf	1349947 e575ddea1dbd118c389bb0d81e99a3af6a0e7d26	no	3
Warnings:					
Information:					
			Total Files Size (in bytes):	1662704	

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.

PTO/SB/30EFS (02-18)
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 contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	15/309,612	Filing Date	2016-11-08	Docket Number (if applicable)	4675.1002BS	Art Unit	3685
First Named Inventor	Reginald Middleton			Examiner Name	James D. Nigh		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

- ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
- ☐ Other _____

☒ Enclosed

- ☒ Amendment/Reply
- ☐ Information Disclosure Statement (IDS)
- ☐ Affidavit(s)/ Declaration(s)
- ☐ Other _____

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____ (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

☒ **The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 504888

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature

Applicant Signature

PTO/SB/30EFS (02-18)
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 contains a valid OMB control number.

Signature of Registered U.S. Patent Practitioner			
Signature	/Misung Lee/	Date (YYYY-MM-DD)	2021-07-27
Name	Misung Lee	Registration Number	78307

This collection of information is required by 37 CFR 1.114. 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.

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

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 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 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.

REMARKS

Reconsideration and allowance in view of the foregoing amendments and the following remarks are respectfully requested.

Claims 1, 3-6, 9, 12, 15-17, 20, 23, 24, 26, 28, 29, 31 and 32 were pending. **Claims 1, 3-6, 9, 12, 15-17, 20, 23, 24, 26, 28, 29, 31 and 32** were rejected under 35 U.S.C. § 101. **Claims 12, 15-17, 23 and 32** were rejected under § 35 U.S.C. § 112(b). **1, 3-6, 9, 12, 15-17, 20, 23, 24, 26, 28, 29, 31 and 32** were rejected under 35 U.S.C. § 103. Upon entry of the amendment, **Claims 1, 12, and 24** are currently amended, **Claim 32** is currently canceled without prejudice or disclaimer, and new **Claim 33** is presented. Support for the amendments to independent **Claims 1, 12, and 24** and new **Claim 33** can be found, at least at, paragraphs [0010], [0011], [0016], [0060]-[0063], [0101], [0324], [0332], [0338] and [0339] of the U.S. Patent Application Publication. No new matter is added.

Favorable consideration is respectfully requested.

EXAMINER INTERVIEW SUMMARY

The courtesy and cooperation shown by Examiner Nigh during the telephone interview of May 6, 2021, are appreciated. During the interview, multiple proposals/amendments to address the rejections under 35 U.S.C. §§ 101 and 103 were discussed. Further, no formal agreement is believed to have been reached regarding the allowability of the claims. The claims have been amended herein based on the discussion during the interview. Consideration of the presented claim amendments and the accompanying remarks is respectfully requested.

CLAIM REJECTION UNDER 35 U.S.C. § 112(b)

Claims 12, 15-17, 23 and 32 *are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as allegedly being indefinite for failing to particularly point out and distinctly claim*

the subject matter which the inventor or a joint inventor (or for applications subject to pre-AIA 35 U.S.C. 112, the applicant), regards as the invention.

Without conceding the propriety of the rejection, but rather as a cooperative effort to move this application to allowance, Applicant is currently amending **Claim 12** and canceling **Claim 32** to address the rejection.

Accordingly, it respectfully requested that the rejection under 35 U.S.C. 112(b) to the claims be reconsidered and withdrawn.

CLAIM REJECTION UNDER 35 U.S.C. § 101

***Claims* 1, 3-6, 9, 12, 15-17, 20, 23, 24, 26, 28, 29, 31 and 32** *are rejected under 35 U.S.C. § 101 as allegedly being directed to an abstract idea without significantly more.*

Applicant traverses the rejection, and respectfully requests that the rejection be reconsidered and withdrawn. Among independent **Claims 1, 12, and 24**, Applicant will discuss **Claim 24** as being representative, but only to the extent that similar features are recited in all three independent claims. Applicant submits that the scope and features of the independent claims are not identical.

The "2019 Revised Patent Subject Matter Eligibility Guidance" (hereafter "Revised Guidance"), effective by the USPTO as of January 7, 2019, has been issued and revised procedures for determining whether a patent claim or patent application claim is directed to a judicial exception and has explained that a patent claim or patent application claim that recites a judicial exception is not directed to the judicial exception if the judicial exception is integrated into a practical application of the judicial exception. Further, the "October 2019 Patent Eligibility Guidance Update" (hereafter "Update"), effective by the USPTO as of October 17, 2019, has been issued.

The Revised Guidance and the Update instruct the Examining Corps to first determine whether claims are directed to one of four statutory categories of invention. If the claim does fall within one of

the statutory categories, the Examining Corps is instructed use the analysis, as explained below.

STEP 1 – DETERMINE WHETHER THE CLAIMS ARE DIRECTED TO ONE OF FOUR STATUTORY CATEGORIES OF INVENTION

In Step 1, a determination is made as to whether the claim is directed to a process, machine, manufacture, or composition of matter. In the present application, there is no dispute that Step 1 has been met as **Claim 24** is directed to a method which is one of four statutory categories of invention. As **Claim 24** is directed to a statutory category, analysis under Step 2 follows, as described below.

STEP 2A – PRONG 1: "WHETHER THE CLAIM RECITES A JUDICIAL EXCEPTION"

Prong 1 of Step 2A of the analysis in Revised Guidance instructs USPTO Examiners should evaluate "whether the claim recites a judicial exception, i.e., an abstract idea, a law of nature, or a natural phenomenon," and "[t]o determine whether a claim recites an abstract idea in Prong One, examiners are now to: (a) Identify the specific limitation(s) in the claim under examination (individually or in combination) that the examiner believes recites an abstract idea; and (b) determine whether the identified limitation(s) falls within the subject matter groupings of abstract ideas." Further, Prong 1 of Step 2A of the analysis states, the abstract idea exception includes the following groupings of subject matter, when recited as such in a claim limitation(s) (that is, when recited on their own or per se):

> (a) Mathematical concepts— mathematical relationships, mathematical formulas or equations, mathematical calculations;
>
> (b) Certain methods of organizing human activity—fundamental economic principles or practices (including hedging, insurance, mitigating risk); commercial or legal interactions (including agreements in the form of contracts; legal obligations; advertising, marketing or sales activities or behaviors; business relations); managing personal behavior or relationships or interactions between people (including social activities, teaching, and following rules or instructions); and
>
> (c) Mental processes—concepts performed in the human mind (including an observation, evaluation, judgment, opinion).

Turning to the Office Action, at pages 28-29, it is alleged that:

> The claim falls within two groupings of abstract ideas involving the ***organizing of human activity*** as indicated in the 2019 Revised Patent Subject Matter Eligibility Guidance, one of which is the processing of ***a payment between two parties which falls under the category of a fundamental economic practice***. As the claim also recites that the transaction requires particular signatures of the intermediary and the first client the claim can also be viewed as falling within the category of a commercial/legal interaction involving a contract involving terms including principal amounts, references to data sources and expiration of the terms i.e. requiring that the contract be consummated within a specified period of time that result in the creation of a disbursement transaction record including amounts, values, signatures and commitment inputs that are then published to both parties to the contract. The disclosure itself recites at paragraph 108 that "The invention pertains to agreements among distinct parties that contemplate transfer of title to property, as well as any industry where that may be of value or importance" and clearly ***falls within the grouping of commercial/legal interactions under the groupings***. The encryption is being claimed at a generally high level and only serves to add a ***mathematical relationship*** to the claim as it is directed towards another one of the groupings in the 2019 PEG. ***Many of the operations can also be performed by human beings using pen and paper such as obtaining terms, creating records and performing transactions***. Therefore under the analysis made under prong one of step 2A the claim is determined to be ineligible.

Applicant respectfully disagrees. Nevertheless, without conceding the propriety of the rejection, but rather as a cooperative effort to expedite the prosecution of this application to allowance, Applicant has amended **Claim 24** to address the rejection.

Currently amended **Claim 24** recites (emphasis added):

> A method for processing a transaction between a first client device and a second client device via a transfer mechanism, the transfer mechanism comprising **a decentralized digital currency comprising a distributed ledger** that is accessible via a computer network by a computer device, the first client device, and the second client device, respectively, the method comprising:
>
> storing a first asymmetric key pair in a first memory, the first asymmetric key pair comprising a first private key and a first public key;
>
> storing a second asymmetric key pair a second memory, the second asymmetric key pair comprising a second private key and a second public key;
>
> storing a third asymmetric key pair in the second memory, the third key pair comprising a third private key and a third public key;

storing a fourth asymmetric key pair in a third memory, the fourth asymmetric key pair comprising a fourth private key and a fourth public key;

transmitting terms from one of the first or second client device via a first network interface, the terms comprising:

at least one of a first principal data or a second principal data;

a reference to at least one of a first data source or a second data source; and

an expiration timestamp;

receiving the terms at the computer device via a second network interface;

reading the first private key from the first memory;

computing a first cryptographic signature from the first private key;

creating a first principal transaction data record comprising:

a first principal output comprising the first principal data; and

the first cryptographic signature;

creating a first principal transaction by submitting the first principal transaction data record to the transfer mechanism;

reading the second private key from the second memory;

computing a second cryptographic signature from the second private key;

creating a commit transaction data record comprising:

a first principal input for receiving the first principal data from the first principal transaction;

a commit output comprising a commit data; and

the second cryptographic signature;

creating the commit transaction by submitting the commit transaction data record to the transfer mechanism;

retrieving a value data from the first data source;

reading the third private key from the second memory;

computing a third cryptographic signature from the second private key;

creating an inchoate data record comprising:

a commit input for receiving a commit data from the commit transaction;

one or more output data obtained from at least one of the first principal data or the second principal data and the value from the first data source; and

the third cryptographic signature;

publishing the inchoate data record;

reading the inchoate data record;

signing the inchoate data record and saving a copy of the inchoate data record on at least one of the first client device or the second client device;

reading the fourth private key from the third memory;

computing a fourth cryptographic signature from the fourth private key;

creating a complete data record comprising:
the commit input;
the one or more output data;
the third cryptographic signature; and
the fourth cryptographic signature;

creating the transaction by broadcasting the complete data record for transmitting and receiving among network participants in the computer network for recording in the distributed ledger; and

verifying, via at least one of the computing device, the first client device, or the second client device, the recording of the complete data record in the distributed ledger by observing an external state,

wherein the distributed ledger enables processing the transaction between the first client device and the second client device without the need for a trusted central authority.

In contrast to the above allegations by the Office Action, currently amended **Claim 24** is directed to a specific computing device for enabling increased security for either party entering into the transaction via a decentralized digital currency of the transfer mechanism, which comprises a distributed ledger, without the need for a trusted central authority. Furthermore, the computing device as recited in amended **Claim 24** participates in the transaction, but the computing device alone cannot control disposition. Instead, the computing device only effects the transaction between the client devices in conjunction with the participation of one of the first or second client device and only in a fashion that was previously and unanimously agreed upon by both parties, and either the first and/or second client device is responsible for ultimately administering the transaction via the decentralized digital currency which comprises a distributed ledger.

The claimed decentralized digital currency prevents the computer device from being commandeered to effect transaction not contemplated by at least one of the first or second client device. As argued in the previously filed Response, the computer device is a distributed participant that works in connection with the first and second client device in a decentralized role (the antithesis of a centralized actor, authority or entity), ensuring not only that it is not centralized, but enabling transactions without involvement of centralized, costly third-party intermediaries who traditionally may

otherwise be required, and without traditional exposure to counterparty risk. Further, as described in paragraph [0339] of the present application, "transaction" is to refer to the part of a ledger or block within a distributed ledger comprising the "transaction record" wherein the "transaction record" is a data structure describing a transaction and submitted to a transfer mechanism to effect a transaction. The claimed computer instructions which verify and execute its terms upon the occurrence of the predetermined events do not correspond to "fundamental economic practice" or "a commercial/legal interaction," as alleged by the Office Action. It is respectfully submitted that the feature of amended **Claim 24** is implemented on the decentralized digital currency, distributed ledger that is not to be a "fundamental" economic practice or "a commercial/legal interaction."

In the decision of *Ex parte Steven Charles Davis*, No. 2019-004127 (P.T.A.B. Aug. 19, 2020), it was determined that the claimed subject matter involves steps and elements that could not be performed by a human mind, even with the aid of pen and paper based on the following reasons:

> Appellant does, however, present arguments that "the claims recite the explicit use of a number of technologies that cannot be performed by human work or mentally, even given a significant amount of time" (Reply Br. 3), because "digital signatures are of sufficient data size and complexity to not be understood by human mental work, let alone verified through the use of a public key and overly complex (by design) signature algorithms" (Reply Br. 3). In this light, with regard to the claims reciting a mental process capable of being performed in the human mind, or with pen and paper, Appellant's arguments (seeReply Br. 2–4) are persuasive…
>
> …In this light, with regard to the claims reciting a mental process capable of being performed in the human mind, or with pen and paper, Appellant's arguments (seeReply Br. 2–4) are persuasive. As stated by Appellant:
>
> > In addition, transaction messages are processed in speeds that have to be measured in nanoseconds for network reliability and due to the overwhelming number of transaction processed each day, necessitating the use of specialized computer systems, which is impossible to replicate through human mental work. Thus, specially configured computer systems are used in the claimed invention, which uses technology in an unconventional way to implement the steps recited in the present claims.

Similar to the decision of *Ex parte Steven Charles Davis*, it is respectfully submitted that the use of the distributed ledger differs from a generic computer component that performs processes which could be performed in the mind or using pen and paper. For example, the distributed nature of the distributed ledger requires a copy of the ledger to be stored on different nodes across the network. In particular, currently amended **Claim 24** recites "***signing the inchoate data record and saving a copy of the inchoate data record on the at least one of the first client device or the second client device***," and "***creating the transaction by broadcasting the complete data record for transmitting and receiving among network participants in the computer network for recording in the distributed ledger; and verifying, via at least one of the computing device, the first client device, or the second client device, the recording of the complete data record in the distributed ledger by observing an external state***." A person cannot do the above simply in their mind or simply using pen and paper and the claimed features associated with the distributed nature of the distributed ledger technology do not fall into "organizing of human activity" as alleged by the Office Action.

At least in view of the current amendments, Applicant respectfully submits that currently amended **Claim 24** does not fall into "organizing of human activity" or any of three groupings of abstract ideas, and that Prong 1 of Step 2A must be answered "NO."

STEP 2A – PRONG 2: "WHETHER THE JUDICIAL EXCEPTION IS INTEGRATED INTO A PRACTICAL APPLICATION"

Prong 2 of Step 2 of the analysis in Revised Guidance instructs that:

> [E]xaminers should evaluate ***whether the claim as a whole integrates the recited judicial exception into a practical application of the exception***. A claim that integrates a judicial exception into a practical application will apply, rely on, or use the judicial exception ***in a manner that imposes a meaningful limit on the judicial exception, such that the claim is more than a drafting effort designed to monopolize the judicial exception***. When the exception is so integrated, then the claim is not directed to a judicial exception (Step 2A: NO) and is eligible.

Further, Prong 2 of Step 2 of the analysis states that:

> Examiners evaluate integration into a practical application by: (a) Identifying whether there are any additional elements recited in the claim beyond the judicial exception(s); and (b) ***evaluating those additional elements individually and in combination to determine whether they integrate the exception into a practical application, using one or more of the considerations***...

Examples in the Revised Guidance that are indicative that an additional element (or combination of elements) may have "integrated the exception into a practical application" include (*emphasis added*):

> - An additional element reflects ***an improvement in the functioning of a computer, or an improvement to other technology or technical field***;
> - An additional element that applies or uses a judicial exception to effect a particular treatment or prophylaxis for a disease or medical condition;
> - An additional element implements a judicial exception with, or uses a judicial exception in conjunction with, a particular machine or manufacture that is integral to the claim;
> - An additional element effects a transformation or reduction of a particular article to a different state or thing; and
> - An additional element applies or uses the judicial exception in ***some other meaningful way beyond generally linking the use of the judicial exception to a particular technological environment, such that the claim as a whole is more than a drafting effort designed to monopolize the exception.***

The Office Action, at pages 27-28, further alleges:

> The structural elements in the claim are limited to what is described as a "transfer mechanism", three memories and two network interfaces along with recitations of first and second clients in the preamble. The claim also recites the capability of encryption by taking a private key and computing a cryptographic signature. In reviewing the written disclosure at paragraphs 52-53, 106 and 113 the memory and network interface are described in a manner that includes no technological improvement to the functioning of the memory and network interface and only describes a particular technological environment for which an intermediary described in paragraph 113 as a "facilitator" is linked. With regard to the encryption capabilities no particular algorithm for computing a signature is described in the written disclosure beyond the recitations at pages 17, 18 and 28 that in order to consummate a transaction that a plurality of signatures are required and the function is described at a generally high level by the

> written disclosure such that in the broadest reasonable interpretation the claim scope encompasses encryption that could be performed by human beings. Even if a computer calculation of the signature were inferred from the claim the written disclosure relies on prior art signature calculation mechanisms such as multisignature transactions (see footnote 2 of page 4 of the written disclosure) or P2SH (97 and 104 of the written disclosure) and therefore do not constitute any technological improvement to the functioning of the computer itself. With regard to the two clients paragraph 110 in describing the client also describes a generic computing device with no technological improvement. The transfer mechanism per paragraphs 53, 54 and 96 are not elements of physical structure but instead are protocols involving at least decentralized currency ("Where a decentralized digital currency [e.g., the Bitcoin protocol, the Ethereum protocol, or similar] is used as the transfer mechanism…", 96) but **per paragraph 49 can also involve centralized currency and the broadest reasonable interpretation of the term transfer mechanism can be viewed as any form of monetary exchange scheme.** If the combination of transfer mechanism, memory, network interfaces and two clients are considered there is no meaningful technological contribution being made in the form of a combination of elements as the transfer mechanism and clients merely represent the computer equivalents of two parties to a contract in which an intermediary is used through the network interfaces and therefore the combination as a whole is merely a mechanism for linking the abstract idea to a particular technological environment. Therefore under prong two of Step 2A no practical application of the abstract idea is present in the claim and the result of the analysis is that the claim is still ineligible.

Applicant respectfully disagrees.

In contrast to the above emphasized allegations of the Office Action, as set forth above, currently amended **Claim 24** recites, in part, "***creating the transaction by broadcasting the complete data record for transmitting and receiving among network participants in the computer network for recording in the distributed ledger; and verifying, via at least one of the computing device, the first client device, or the second client device, the recording of the complete data record in the distributed ledger by observing an external state***."

In accordance with the current amendments, the transfer mechanism of **Claim 24** comprises a distributed ledger achieving an enhanced security for either party entering into the transaction via the decentralized digital currency of the transfer mechanism, without requiring **a trusted central authority**,

because the decentralized digital currency of the transfer mechanism, which includes a distributed ledger enabling the transactions being validated by a number of participants in the network before the transaction actually occurs and being recorded on the distributed ledger. As described in paragraph [0339] of the present application, "transaction" is to refer to the part of a ledger or block within a block chain comprising the "transaction record" wherein the "transaction record" is a data structure describing a transaction and submitted to a transfer mechanism to effect a distributed ledger transaction.

In 2019 PEG Example 41 ("Example 41"), issued January 7, 2019, the combination of additional elements use the mathematical formulas and calculations in ***a specific manner that sufficiently limits the use of the mathematical concepts to the practical application of transmitting the ciphertext word signal to a computer terminal over a communication channel****, and the mathematical concepts are* ***integrated into a process that secures private network communications****.* Therefore, in Example 41, a ciphertext word signal can be transmitted ***between computers of people who do not know each other or who have not shared a private key between them in advance of the message being transmitted***, where the security of the cipher relies on the difficulty of factoring large integers by computers, and thus the claim is not directed to the recited judicial exception (a claim drawn to a "method for establishing cryptographic communications" was decided to be patent eligible).

Similar to Example 41, amended **Claim 24** is directed to a specific method for enabling increased security for either party entering into the transaction *with little trust or no trust in each other* via the decentralized digital currency of the transfer mechanism, *without involving costly third-party intermediaries who traditionally may otherwise be required, and traditional exposure to counterparty risk* (see paragraph [0025] of the U.S. Patent Application Publication). At least the above emphasized features of amended **Claim 24** solve a technical problem of conventional transaction that requires involvement of expensive third-party intermediaries or a trusted central authority. In contrast to the

allegation of "***the function [being] described at a generally high level by the written disclosure such that in the broadest reasonable interpretation the claim scope encompasses encryption that could be performed by human beings***," as alleged by the Office Action, Applicant submits that amended **Claim 24** is directed to improvements in processing transaction technology, particularly, via a transfer mechanism comprising a decentralized digital currency which comprises a distributed ledger with enhanced security. At least the above emphasized features of amended **Claim 24**, for example, permits providing enhanced security for either party entering into the transaction via the decentralized digital currency of the transfer mechanism, without requiring a trusted central authority, because a distributed ledger requires that transactions are validated by a number of participants in the network before the transaction actually occurs and is recorded on the distributed ledger. In this regard, a part or whole of paragraphs [0010] and [0011] of the U.S. Patent Application Publication are reproduced below:

> [0010] For the purposes of illustration by way of non-limiting example, ***those particular decentralized digital currencies generally operate by maintaining a whole or partial history or "ledger" (sometimes referred to as a "block chain") of all transactions that have been "validated" by a consensus of network participants.*** With few exceptions beyond the scope of the invention, transactions function roughly as follows.<2 >A transaction comprises at least one input and at least one output. The input comprises an input "script", which comprises an ordered set of well-defined executable operations. The output comprises an output script, which comprises a second ordered set of such operations. A new (child) transaction comprises an input whose input script is combined with the output script from an existing (parent) transaction in a predictable way. ***The new transaction is considered valid if a majority of network participants agree that the combination, when evaluated according to a predetermined set of rules, produces an anticipated state or result…***
>
> [0011] More specifically, the entity seeking to submit a new transaction to the ledger transmits (or "broadcasts") a transaction record comprising the details of the desired transaction to a number of network participants then known to the entity (or "peers"). Those peers typically attempt to independently validate the transaction record. If successful, they rebroadcast the transaction record to their peers, and so on. ***Eventually the transaction record is received by a network participant who is configured to effect the transaction by including the***

transaction record in the ledger (i.e., in a valid "block"); see more detailed description below).

In particular, the claimed "*creating the transaction by broadcasting the complete data record for transmitting and receiving among network participants in the computer network for recording in the distributed ledger; and verifying, via at least one of the computing device, the first client device, or the second client device, the recording of the complete data record in the distributed ledger by observing an external state"* enables the transaction data record being made available for verification to all participants of the network, who can independently verify the transaction data record before the transaction is actually effected when one participant adds the transaction to the distributed ledger. Therefore, involvement of expensive third-party intermediaries can be avoided, and counter party risk can be mitigated from enabling transactions among multiple parties.

Accordingly, Applicant respectfully submits that amended **Claim 24** is directed to an improvement in technology, similar to eligible claims in *McRO or DDR*, and is integrated into a practical application of the judicial exception, as required by the Revised Guidance.

Furthermore, in contrast to the allegation that the function is described at a generally high level that could be performed by human beings as alleged by the Office Action, amended **Claim 24** recites "the transfer mechanism comprising a decentralized digital currency." It is respectfully submitted that, by definition, participation with a ***decentralized*** digital currency comprising ***a distributed ledger*** is done so with a device and in a manner in which human beings have never acted previously. A decentralized currency that exists solely outside of that context (e.g., one that is devoid of a network of participants) would be worthless, which is why the claims are limited to decentralized digital currencies, not other types of currencies. Further, decentralized digital currencies are worthless without decentralized participants and a distributed physical data record of transactions that record cryptographic solutions as a means of proving authority to effect transfers. Prior to the present application, no human had demonstrated application of this technology to accomplish the goals of the present application at all,

much less in the manner in which the present application presents. Further, before the present application, it was physically impossible for an intermediary (human or otherwise) to control disposition without additional participants. Further still, nowhere does the present application suggests that conventional centralized transfer mechanisms can achieve improvements of the technologies enabled by amended **Claim 24** as implemented on the decentralized digital currencies, a distributed ledger.

Amended **Claim 24** is directed to a specific method for data processing implemented on the *decentralized digital currency* but not on the centralized currency. The computer device as recited in amended **Claim 24** participates in the transaction but the computer device alone does not control disposition. Instead, the computer device only effects a transaction in conjunction with the participation of one of the first or second clients and either the first or second client is responsible for ultimately administering the transaction via the *decentralized digital currency.* The claimed decentralized digital currency prevents the computer device from being commandeered to effect the transaction not contemplated by at least one of the first or second client device. As such, by definition, the computer device is a distributed participant that works in connection with the first and second client devices, but that does not make it centralized. For example, paragraphs [0009], [0015], [0016], and [0018] of the U.S. Patent Application Publication state, in part or whole (emphasis added):

> [0009] Decentralized digital currencies (or so-called "cryptocurrencies")—technologies that promise ***tightly-controlled asset creation*** coupled with the ability to ***transfer control or ownership of those assets computationally when rigorously-defined criteria are met***, ***with little-or-no dependency on third party intermediaries***, and with very low transaction costs compared to traditional mechanisms—are relatively new creatures. ***The Bitcoin protocol*** and progeny (Ethereum, Litecoin, etc.) are ***one such class of technologies*** that have recently enjoyed meteoric rises in popularity (and valuation).
>
> [0015] … While this section often refers to "***Bitcoin***" by name, the description is accurate for nearly ***all of the decentralized digital currencies*** currently known in the art…
>
> [0016]… A novel solution accomplishes this ***without any trusted central authority: maintenance of the block chain is performed by a network***

> ***of communicating nodes running bitcoin software***…
>
> [0018] … Ownership of bitcoins implies that a user can spend bitcoins associated with a specific address. To do so, a payer must digitally sign the transaction using the corresponding private key. Without knowledge of the private key the transaction cannot be signed and bitcoins cannot be spent. The network verifies the signature using the public key. If the private key is lost, the bitcoin network will not recognize any other evidence of ownership; the coins are then unusable, and thus effectively lost. For example, in 2013 one user said he lost 7,500 bitcoins, worth $7.5 million at the time, when he discarded a hard drive containing his private key…

Furthermore, paragraph [0025] of the U.S. Patent Application Publication states:

> [0025] The invention pertains to ***systems and methods enabling parties with little trust or no trust in each other to enter into and enforce agreements conditioned on input from or participation of a third party, over arbitrary distances, without special technical knowledge of the underlying transfer mechanism(s), optionally affording participation of third-party mediators, substitution of transferors and transferees, term substitution, revision, or reformation, etc. Such exchanges can occur reliably without involving costly third-party intermediaries who traditionally may otherwise be required, and without traditional exposure to counterparty risk***.

The above recited critical features of *decentralized digital currencies, a distributed ledger,* afford the novelty of a participating facilitator without also allowing that the computer device to control dispositions (**without the need for a trusted central authority)**. Nowhere does the present application suggest that conventional transfer mechanisms can stand in for decentralized digital currencies.

Also, paragraph [0029] of the U.S. Patent Application Publication states:

> [0029] Combinations are possible. For example, Party A accepts Australian dollars (AUD), but prefers USD, and wants to hedge against volatility of AUD in USD. One embodiment of the invention allows Party A to swap exposure to USD in BTC with Party B, and simultaneously swap exposure to BTC in AUD with Party C over a similar time period, thereby synthesizing a hedge against AUD in USD. The invention is not limited such that Party B and Party C are distinct parties (they could be the same), nor is it limited such that such that Party A must conduct two separate trades. In addition, various embodiments of the invention allow the parties to perform these types of transactions without maintaining currency deposits or making currency purchases or

exchanges.

As set forth above, paragraph [0029] of the U.S. Patent Application Publication describes how to synthesize a swap transaction using the features as described in the present application. It does not contemplate removing the characteristics of decentralized digital currencies that afford the aforementioned features. Implementing the benefits of the present application would not be possible using conventional transfer mechanisms, which all involve third party intermediaries who temporarily control disposition of transfers. That is, the present application implemented on the decentralized digital currencies including a distributed ledger affords transactions between participants in the network where no intermediary has an opportunity to behave badly or incompetently, thereby mitigating counterparty risk.

Furthermore, the decision of *Ex parte Steven Charles Davis*, it was further determined that the claimed subject matter directed to an improvement in technology based on the following reasons:

> Appellant disagrees, and contends that the claims "are directed to an inventive concept that is an unconventional combination of a traditional payment processing network and a blockchain network" (Appeal Br. 8); and (ii) that that inventive concept results in a technical improvement (see Appeal Br. 10).7 Appellant argues that "the claims recite the explicit use of a number of technologies that cannot be performed by human work or mentally, even given a significant amount of time" (Reply Br. 3), and require "using both networks [i.e., payment network and blockchain] with the computer system [to ensure] that the party in the submitted transaction message was a party to the blockchain transaction" (Reply Br. 3). Appellant further contends the "claims, even if generic computer hardware is used, are still directed to an ordered combination that recites an inventive concept that is unconventional and a solution to a technical problem" (Appeal Br. 11).
>
> We agree. Appellant identifies persuasively how the Specification sets forth an improvement in technology, and how the claims recite that improvement.
>
> Claims 1–16 recite an ordered combination of elements that: (i) are an improvement to blockchain or other technology or technical field (see MPEP § 2106.05(a)); and (ii) include meaningful limitations on the recited abstract idea (see MPEP § 2106.05(e)). See also Guidance, 84 Fed. Reg. at 55; Ex Parte Rios, Appeal No. 2019-004130, at 13 (PTAB Feb. 26, 2020) (concluding that ***a multi-currency payment transaction platform using different currencies integrate the recited judicial***

exception of a fundamental economic practice into a practical application.)

Similar to the above decision of *Ex parte Steven Charles Davis*, and further similar to *BASCOM Global Internet Services, Inc. v. AT&T Mobility LLC* (Fed. Cir. June 27, 2016), amended **Claim 24** recites an ordered combination of elements (*e.g.* asymmetric key pairs, data feeds, scripts, and distributed ledger, etc.) in such a fashion that enables conducting a bilateral trustless transfer of conditional value with the tools and information at hand that is an improvement to computer technical field or other technology and an inventive concept that is unconventional and a solution to a technical problem.

Accordingly, Applicant respectfully submits that amended **Claim 24** is directed to an improvement in technology and is integrated into a practical application of the judicial exception, as required by the Revised Guidance.

At least in view of the current amendments, Applicant respectfully submits that amended **Claim 24** does not fall into any of the three groupings of abstract ideas, and even if **Claim 24** recites an abstract idea, **Claim 24** integrates the recited judicial exception into a practical application of the exception, and that Prong 2 of Step 2A must be answered "YES."

STEP 2B - PART 2 OF THE "TWO-PART ANALYSIS FOR ABSTRACT IDEAS"

Even if a claim has been determined to be directed to a judicial exception under revised Step 2A, Step 2B of the analysis in Revised Guidance instructs "examiners should then evaluate the additional elements individually and in combination under Step 2B to determine whether they provide an inventive concept (i.e., whether the additional elements amount to significantly more than the exception itself)."

Still, even if evidence were to be offered, Applicant submits that amended **Claim 24** recites significantly more than the alleged abstract idea.

In the rejection of previously-presented **Claim 24**, the Office Action, at pages 5, 33, and 34, alleges:

> Applicant's further argument (pages 34-37 of remarks) with regard to the present rejection under section 101 that the claims amount to significantly more than the abstract idea under Step 2B has been fully considered but is not persuasive. The arguments are substantially similar to those presented regarding Prong Two of Step 2A and Examiner does not see where Applicant has actually pointed to any technological improvement that is taking place but instead is pointing to ***an improvement that is related to conducting business using the claimed invention.*** However ***an improvement that is directed entirely towards a business objective*** must be viewed as being part of the abstract idea itself and does not serve under Step 2B to form something that can be viewed as contributing significantly more to the claim then the abstract idea itself. Therefore this argument is also unpersuasive.
>
> However in the instant claims ***the recited operations of transferring payments and utilizing trusted intermediaries in making a payment as part of a contractual relationship are all operations that have previously been done by human beings in the same manner being claimed***.

Applicant disagrees and submits that amended **Claim 24** recites significantly more than the alleged abstract idea.

As discussed above, it is respectfully submitted that the claimed combination improves a transaction technology, via a transfer mechanism comprising a decentralized digital currency which comprises a distributed ledger with enhanced security and mitigated third party risks. At least the above emphasized features of amended **Claim 24**, for example, permits providing an enhanced security for either party entering into the transaction via the decentralized digital currency of the transfer mechanism, **without requiring a trusted central authority**, because the decentralized digital currency of the transfer mechanism, which includes a distributed ledger, requires that transactions are validated by a number of participants in the network before the transaction actually occurs and is recorded on the distributed ledger. Furthermore, implementing specific improvements achieved by the present application would not be possible using conventional transfer mechanisms which all involve third party intermediaries who temporarily control disposition of transfers. That is, the present application implemented on the decentralized digital currencies affords transactions between parties where no

intermediary has an opportunity to behave badly or incompetently.

Furthermore, in contrast to the allegations by the Office Action, it is submitted that the feature of amended **Claim 24** is implemented on the *decentralized digital currency, a distributed ledger* that is not to be "an improvement that is directed entirely towards a business objective." It is again respectfully submitted that the use of the distributed ledger differs from a generic computer component that performs processes which could be performed in the mind or using pen and paper. For example, the distributed nature of the ledger requires a copy of the ledger to be stored on different nodes across the network. In particular, currently amended **Claim 24** recites "***signing the inchoate data record and saving a copy of the inchoate data record on the at least one of the first client device or the second client device***," and "***creating the transaction by broadcasting the complete data record for transmitting and receiving among network participants in the computer network for recording in the distributed ledger; and verifying, via at least one of the computing device, the first client device, or the second client device, the recording of the complete data record in the distributed ledger by observing an external state***." A person cannot do the above simply in their mind or simply using pen and paper and the claimed features associated with the distributed ledger do not correspond to "all operations that have previously been done by human beings in the same manner being claimed" as alleged by the Office Action.

Therefore, currently amended **Claim 24** recites specific improvements over prior methods, resulting in an enhanced transfer technology implemented on a decentralized digital currency, and does not direct to "a generic computing device with no technological improvement," as alleged by the Office Action.

For at least the foregoing reasons, amended **Claim 24** recites "significantly more" than the alleged abstract idea. Independent **Claims 1 and 12** are similarly amended to recite such feature.

Accordingly, Step 2B is answered "Yes" and all claims are patent eligible. Reconsideration and withdrawal of the rejection are thus respectfully requested. Applicant respectfully requests that the rejection of **Claims 1, 3-6, 9, 12, 15-17, 20, 23, 24, 26, 28, 29, 31, and 33** under 35 U.S.C. § 101 be reconsidered and withdrawn.

CLAIM REJECTION UNDER 35 U.S.C. § 112

Claims 12, 15-17, 23 and 32 *are rejected under 35 U.S.C. § 112(b) or 35 U.S.C. § 112 (pre-AIA), second paragraph, as allegedly 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.*

Without conceding the propriety of the rejections, but rather as a part of cooperative efforts to expedite the prosecution of this application to allowance, Applicant is currently amending **Claims 1, and 3-6**. Accordingly, at least in view of the current amendments, Applicant, therefore, respectfully requests the reconsideration and withdrawal of rejection under 35 U.S.C. § 112(b).

CLAIM REJECTIONS UNDER 35 U.S.C. § 103

***Claims* 1, 3-6, 9, 12, 15-17, 20, 23, 24, 26, 28, 29, 31 and 32** *rejected under 35 U.S.C. § 103 as allegedly being unpatentable over Rosen (U.S. Publication No. 2003/0070080; hereafter "Rosen") and further in view of Feigelson (U.S. Publication No. 2013/0166455; hereafter "Feigelson") in view of Ginter (U.S. Patent Publication No. 2009/0030768, now U.S. Patent No. 7,587,369; hereafter "Ginter")*

Applicant traverses the rejection, and respectfully requests that the rejection be reconsidered and withdrawn.

In the rejection of previously presented **Claim 24**, in Response to Arguments section of the Office Action, at pages 5-6, it is alleged that:

> Examiner would reiterate that as the claim is directed towards a role of an intermediary that there is nothing in the claim that would alter the function of the intermediary based on whether a centralized or decentralized currency were being used and Applicant has presented nothing more than a conclusory argument. Furthermore there is nothing within the Rosen reference that disparages the use of a

> decentralized currency and in order to "teach away" from the claimed invention the reference would have to make a statement to the effect that precludes or disparages the use of cryptocurrency (In re Fulton, 391 F.3d 1195, 1201, 73 USPQ2d 1141, 1146 (Fed. Cir. 2004), MPEP § 2123, 2141.02 (VI)). Without such a statement present in the Rosen reference itself the allegation that Rosen "teaches away" from the use of decentralized currency must be held as unpersuasive.

As acknowledged by the Office Action, at page 37, "Rosen, while disclosing electronic money (Abstract), does not explicitly disclose wherein the transfer mechanism comprises a decentralized currency." The Office Action further alleges that "Feigelson teaches wherein the transfer mechanism comprises a decentralized currency (0050-0051)" and "it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the electronic monetary system of Rosen with the creation and use of digital currency of Feigelson for the purpose of maintaining secrecy of information in order to control its value (0003)."

Applicant respectfully disagrees and submits that Rosen and Fergerson are not combinable and there is no motivation to combine Rosen and Fergerson for one of ordinary skill in the art.

Rosen identifies intermediaries who store and control currency (value) as agents or intermediaries or promissories. For example, Rosen describes various scenarios, all of which involve such controlling intermediaries like deposit banks, correspondent banks, participating banks, issuing banks, and clearing banks (see Rosen, at paragraph [0026]). Further, Rosen describes mechanisms using cryptography managed by a central authority for the sole purpose of authentication (see Rosen, paragraph [0191]). Further still, Rosen describes trusted agents 2, 4 for both the customer and merchant (see Rosen, paragraph [0630]).

From the above and other descriptions in Rosen, it is summarized that Rosen requires (i) a trusted centralized facilitator (or intermediary), (ii) a trusted agent for each of merchant and customer, and (iii) a certificate central authority.

Accordingly, Rosen and Fergerson are not combinable. The proposed combination of Rosen

and Feigelson would impermissibly render Feigelson unsatisfactory for its intended purpose because all benefits derived from Feigelson are lost when moving from tokens as described by Feigelson to conventional forms of account as described by Rosen. There is no way to combine Feigelson with Rosen that retains the advantages of Feigelson's disclosure. Therefore, modifying Feigelson by adding features described in Rosen would impermissibly render Feigelson unsatisfactory for its intended purpose of providing security features for the physical devices that carry values. Moreover, the proposed modification would impermissibly changethe principle of operation of Feigelson.

In contrast to **Claim 24**, not only Rosen fails to teach or suggest a method for processing a transaction implemented on decentralized digital currencies, but also *teaches away* the claimed method implemented on the decentralized digital currencies because as discussed above Rosen identifies intermediaries who store and control currency (value) as agents or intermediaries or promissories. For example, Rosen describes various scenarios, all of which involve such controlling intermediaries like deposit banks, correspondent banks, participating banks, issuing banks, and clearing banks, see Rosen, at paragraph [0026]. Rosen's (i) a trusted centralized facilitator (or intermediary), (ii) a trusted agent for each of merchant and customer, and (iii) a certificate central authority disparages or precludes the use of a decentralized currency, and therefore, and "teach away" *teaches away* the claimed method implemented on the decentralized digital currencies.

Applicant further submits that the Office Action's rationale with respect to the rejection of **Claim 24** is based on impermissible hindsight that relies solely upon the disclosed claim elements and advantages of the claimed elements as provided in Applicant's own disclosure as a roadmap for modifying the applied references (in particular, Rosen and Fergerson). The rational is not based on a disclosure or suggestion that is motivated by the references, or that would be suggested based on a review of the references.

That the Office Action is based on impermissible hindsight bias is demonstrated by the assertions in the Office Action that the claims are obvious in view of Rosen and Fergerson. This is at least evidenced by the Office Action's use of Rosen as a reference.

As discussed above, Rosen involves (i) a trusted centralized facilitator (or intermediary), (ii) a trusted agent for each of merchant and customer, and (iii) a certificate central authority disparages or precludes the use of a decentralized currency. That is, Rosen does not concern the computer device which is *a distributed participant* that works in connection with the first and second client device in a decentralized role, ensuring not only that it is not centralized, but enabling transactions *without the need or involvement of centralized, costly third-party intermediaries who traditionally may otherwise be required, and without traditional exposure to counterparty risk*.

Therefore, one of ordinary skill in the art would not look to this assemblage of references, such as (i) a trusted centralized facilitator (or intermediary), (ii) a trusted agent for each of merchant and customer, and (iii) a certificate central authority as described by Rosen, for a solution to a problem involving a distributed ledger that enables processing the transaction between the first client device and the second client device without the need for a trusted central authority as claimed. The fields of endeavor are different. According to MPEP §2145:

> "[a]ny judgment on obviousness is in a sense necessarily a reconstruction based on hindsight reasoning, but so long as it takes into account only knowledge which was within the level of ordinary skill in the art at the time the claimed invention was made and does not include knowledge gleaned only from applicant's disclosure, such a reconstruction is proper." In re McLaughlin, 443 F.2d 1392, 1395, 170 USPQ 209, 212 (CCPA 1971). Applicants may also argue that the combination of two or more references is "hindsight" because "express" motivation to combine the references is lacking.

Further, the U.S. Court of Appeals for the Federal Circuit has instructed that "It is impermissible to use the claimed invention as an instruction manual or 'template' to piece together the teachings of

the prior art so that the claimed invention is rendered obvious." *In re Fritch*, 972 F.2d 1260, 1266 (Fed. Cir. 1992).

Here, even *assuming arguendo* that the proposed combination of the cited references taught the claim elements, the rejection of the present claims is improper because the rejection is founded on knowledge gleaned only from Applicant's disclosures and the proposed combination based on these disparate teachings in the cited references is the product of impermissible hindsight that effectively uses Applicant's disclosure as a blueprint to arrive at the claim.

Nevertheless, without conceding the propriety of the rejection, but rather as part of cooperative efforts to expedite the prosecution of this application to allowance, as set forth above, **Claim 24** is currently amended to recite, in part (emphasis added):

> ***creating the transaction by broadcasting the complete data record for transmitting and receiving among network participants in the computer network for recording in the distributed ledger****; and*
>
> ***verifying, via at least one of the computing device, the first client device, or the second client device, the recording of the complete data record in the distributed ledger by observing an external state,***
>
> ***wherein the distributed ledger enables processing the transaction between the first client device and the second client device without the need for a trusted central authority***.

At least the above features of amended **Claim 24** cannot be taught or even suggested by combining Rosen's (i) a trusted centralized facilitator (or intermediary), (ii) a trusted agent for each of merchant and customer, and (iii) a certificate central authority with any other references.

Further, amended **Claim 24** recites, in part (emphasis added):

> ***signing the inchoate data record and saving a copy of the inchoate data record on the at least one of the first client device or the second client device***...

In the rejection of previously presented **Claim 24**, the Office Action, at page 51, further alleges:

> Rosen discloses creating an inchoate data record comprising: a commit input for receiving a commit data from the commit transaction (0157-0174, 0176-0179, 0193, 0300, 0791-0802)

> Rosen discloses one or more output data obtained from the at least one of the first principal data or the second principal data and the value from the first data source (0157-0174, 0176-0179, 0184, 0535, 0798-0802)
>
> Rosen discloses the third cryptographic signature (0157-0174, 0176-0179, 0193, 0300, 0791-0802)
>
> Rosen discloses publishing the inchoate data record (0157-0174, 0176-0179, 0193, 0300, 0791-0802)
>
> Rosen discloses reading the inchoate data record (0157-0174, 0176-0179, 0193, 0300, 0660, 0662, 0791-0802)

Applicant respectfully disagrees.

For example, Rosen, at paragraphs [0157]-[0159], states (emphasis added):

> [0157] Referring now to FIG. 4, a Transaction money module 4 is shown diagrammatically in block form. Specifically, a Transaction money module 4 has (1) an external interface 30 that interfaces the Transaction money module 4 to the module's data processing means, the input/output means (human interface) and the communications circuitry of the external device; (2) a session manager 31 to control and commit (i.e., finalize) or abort a transaction session; (3) a transactor 32 to manage application functions; and (4) a money holder 38 to contain and manage the electronic representations of money.
>
> [0158] According to the invention, the following application functions may be implemented in the preferred embodiment of the present invention:
>
> [0159] The To Subscriber application 33 performs the function of comparing the owner identification characteristics, such as a user's personal identification number (PIN) and biometrics characteristic (e.g., fingerprint, voiceprint, etc.), that are stored in the memory of the Transaction money module 4, to those of the individual who is attempting to gain access to the Transaction money module 4. ***After the proper ownership is verified, the Transaction money module 4 may be activated, and the user is allowed certain accesses to the Transaction money module's 4 stored contents***. Messages to the subscriber, and subscriber inquiries as to the information contained within the Transaction money module 4 are also handled by this application function.

In Rosen, as shown above, any of contents are stored in the Transaction money module and allowed user accesses to the Transaction money module's stored contents. Rosen does not describe saving a copy of any contents in the client devices. Therefore, Rosen fails to teach or suggest "signing

the inchoate data record and saving a copy of the inchoate data record on the at least one of the first client device or the second client device," as recited in amended **Claim 24**.

Furthermore, Feigelson and Ginter do not compensate for the above deficiencies of Rosen, and nor were Feigelson and Ginter cited for such purposes.

Further still, for at least the same reasons that independent **Claim 24** is patentable over the cited reference, it is respectfully submitted that **Claims 1 and 12** are also patentable, to the extent that **Claims 1 and 12** recite similar features as **Claim 24**. Accordingly, for at least the reasons set forth above regarding **Claim 24**, it is respectfully submitted that Rosen, Feigelson, and Ginter either alone or in combination, fails to teach or suggest all the features of **Claims 1 and 12**; and, therefore, it is respectfully requested that the rejection to independent **Claims 1, 12, and 24** be reconsidered and withdrawn.

Dependent **Claims 3-6, 9, 15-17, 20, 23, 26, 28, 29, and 31** depend, directly or indirectly, from independent **Claims 1, 12 and 24**, respectively. Accordingly, the dependent claims are allowable over the cited references at least by virtue of their dependency from independent **Claims 1, 12 and 24**, as well as the other features recited therein. It is therefore respectfully requested that rejection to **Claims 3-6, 9, 15-17, 20, 23, 26, 28, 29, and 31** under 35 U.S.C. § 103 be reconsidered and withdrawn.

New Claim 33

By this amendment, new **Claim 33** is submitted for examination. **Claim 33** depends from **Claim 24**, and thus, patentable over the cited references for at least the reasons discussed above with respect to **Claim 24**, as well as for the additional features it recites.

Further, in the rejection of previously presented **Claim 24**, the Office Action, at page 49, alleges:

> Rosen discloses transmitting terms from one of the first or second client device via a first network interface (0231-0234) the terms comprising: ***at least one of a first principal data or a second principal data (0165) and a reference to at least one of a first data source or a second data***

> ***source (0159, 1297)*** and an expiration timestamp (Figure 51 in element 1027, 0118, 0261, 0274, 0281) (Examiner notes that the term "expiration timestamp" appears to only be limited to a time at which something expires as a timestamp in typical usage reflects current time, not a past or future time)

Applicant respectfully disagrees and submits that Rosen fails to teach or suggest at least the features as recited in new **Claim 33**.

Paragraphs [0162]-[0172] of Rosen state:

> [0162] The Tran Log Mgr. application 36 provides the management and overseeing of a log that records completed transactions undertaken by the money module. For each completed transfer of electronic money, an illustrative Tran Log records:
> [0163] (1) the type of transfer (i.e., payment, deposit, foreign exchange, etc.),
> [0164] (2) the date of transfer,
> [0165] (3) the amount of transfer,
> [0166] (4) the Issuing Bank 1 identifier
> [0167] (5) the note identifier,
> [0168] (6) the monetary unit,
> [0169] (7) the identifier of the other money module involved in the transaction, and for deposits, withdrawals and loan payments:
> [0170] (8) the bank account number,
> [0171] (9) the bank identifier, and
> [0172] (10) the amount of the transaction.

As shown above, Rosen merely describes a log which records *completed* transactions including the amount of transfer. It is respectfully submitted that any amount of transfer included in the completed transaction of Rosen does not correspond to a first principal data, a first collateral data, a second principal data, or a second collateral data. Further, Rosen does not distinguish principal data or collateral data. Therefore, Rosen fails to teach or suggest "the terms further comprise ***a first collateral data, or a second collateral data***," as recited in new **Claim 33**. Accordingly, it naturally follows that Rosen further fails to teach or suggest "wherein the first principal transaction data record further comprises a first collateral output comprising the first collateral data; wherein the commit transaction data record further comprises a first collateral input for receiving the first collateral data from the first principal transaction; and wherein the one or more output data is obtained from the first principal data

and the first collateral data or the second principal data and the second collateral data, and the value from the first data source," as recited in new **Claim 33**.

Accordingly, favorable consideration of new **Claim 33** is respectfully requested.

CONCLUSION

It is respectfully submitted that the other references in the record do not compensate for the deficiencies of the references utilized in rejecting the pending claims.

It should also be noted that although arguments have been presented with respect to certain claims herein, the recited subject matter as well as various other subject matter and/or combinations of subject matter may be patentable for other reasons. Further, the failure to address any statement by the Examiner herein should not be interpreted as acquiescence or agreement with such statement. Applicant expressly reserves the right to set forth additional and/or alternative reasons for patentability and/or allowance with the present Application or in any other future proceeding, and to rebut any statement presented by the Examiner in this or other papers during prosecution of the present Application.

All objections and rejections having been addressed, it is respectfully submitted that the present application is in condition for allowance, and therefore issuance of a Notice to that effect is earnestly solicited.

Respectfully submitted,

Brundidge & Stanger, PC

Dated: July 27, 2021

/Misung Lee/
Misung Lee
Reg. No. 78,307

Electronic Patent Application Fee Transmittal

Application Number:	15309612
Filing Date:	08-Nov-2016
Title of Invention:	Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers
First Named Inventor/Applicant Name:	Reginald Middleton
Filer:	Misung Lee/Juel Clyne
Attorney Docket Number:	4675.1002BS

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 $0 paid	2253	1	740	740
Miscellaneous:				
RCE- 2ND AND SUBSEQUENT REQUEST	2820	1	1000	1000
		Total in USD ($)		**1740**

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 15/309,612	Filing Date 11/08/2016	☐ 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 $40 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $210 =	
☐ 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	07/27/2021	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 18	Minus	** 30	= 0		x $50 =	0
	Independent (37 CFR 1.16(h))	* 3	Minus	*** 3	= 0		x $240 =	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.	SLIE
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	/RANELL D GRAY/
*** 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.

Notice of References Cited	Application/Control No. 15/309,612	Applicant(s)/Patent Under Reexamination Middleton et al.	
	Examiner JAMES D NIGH	Art Unit 3685	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-20130166455-A1	06-2013	Feigelson; Douglas	G06Q30/06	705/64
*	B	US-20030070080-A1	04-2003	Rosen, Sholom S.	G06Q20/06	713/187
*	C	US-20150287026-A1	10-2015	Yang; Danny	G06Q20/06	705/69
*	D	US-20090025087-A1	01-2009	Peirson, JR.; William Howard	G06Q10/00	726/27
*	E	US-20100138659-A1	06-2010	CARMICHAEL; PAT	H04L9/3263	713/170
*	F	US-20090030768-A1	01-2009	Ginter; Karl L.	G06Q20/04	705/39
*	G	US-7587369-B2	09-2009	Ginter; Karl L.	G06Q20/02	705/75
*	H	US-20150262171-A1	09-2015	Langschaedel; Julian	G06Q20/3825	705/71
*	I	US-9892460-B1	02-2018	Winklevoss; Cameron Howard	G06Q40/04	1/1
*	J	US-20170091750-A1	03-2017	MAIM; Enrico	H04L9/30	1/1
*	K	US-20150120567-A1	04-2015	VAN ROOYEN; Gert-Jan	G06F21/10	705/59
	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	Antonopoulos (“Mastering Bitcoin – Unlocking Digital Crypto-Currencies”, O’Reilly Media, Inc., December, 2014) (Year: 2014)
	V	Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", www.bitcoin.org., 9 pages, March 24, 2009 (Year: 2009)
	W	Ben-Sasson et al., "Zerocash: Decentralized Anonymous Payments from Bitcoin", 2014 IEEE Symposium on Security and Privacy, 16 pages, April 23, 2014 (Year: 2014)
	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.

Bibliographic Data

Application No: 15/309,612

Foreign Priority claimed: ○ Yes ◉ No

35 USC 119 (a-d) conditions met: ☐ Yes ☐ No ☐ Met After Allowance

Verified and Acknowledged: /JAMES D NIGH/ Examiner's Signature | Initials

Title: Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers

---

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
11/08/2016	705	3685	4675.1002BS
RULE			

APPLICANTS

Reginald Middleton, Brooklyn, NY, UNITED STATES

INVENTORS

Reginald Middleton, Brooklyn, NY, UNITED STATES

Matthew Bogosian, Anacortes, WA, UNITED STATES

CONTINUING DATA

This application is a 371 of PCT/US15/29196 05/05/2015

PCT/US15/29196 has PRO of 61990795 05/09/2014

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

03/20/2017

**** SMALL ENTITY ****

STATE OR COUNTRY

UNITED STATES

ADDRESS

BRUNDIDGE & STANGER, P.C.
1925 BALLENGER AVENUE, STE. 560
ALEXANDRIA, VA 22314
UNITED STATES

FILING FEE RECEIVED

$960

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/309,612	Middleton et al.
	Examiner	Art Unit
	JAMES D NIGH	3685

✓	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	10/07/2021								
1	1	=								
	2	-								
2	3	=								
3	4	=								
4	5	=								
5	6	=								
	7	-								
	8	-								
6	9	=								
	10	-								
	11	-								
7	12	=								
	13	-								
	14	-								
8	15	=								
9	16	=								
10	17	=								
	18	-								
	19	-								
11	20	=								
	21	-								
	22	-								
12	23	=								
13	24	=								
	25	-								
14	26	=								
	27	-								
15	28	=								
16	29	=								
	30	-								
17	31	=								
	32	-								
18	33	=								

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/309,612	Middleton et al.
	Examiner	Art Unit
	JAMES D NIGH	3685

CPC						
Symbol					Type	Version
H04L	/	9	/	3247	F	2013-01-01
G06Q	/	20	/	02	I	2013-01-01
G06Q	/	20	/	10	I	2013-01-01
G06Q	/	20	/	065	I	2013-01-01
G06Q	/	40	/	02	I	2013-01-01
H04L	/	29	/	06	I	2013-01-01
H04L	/	2209	/	38	A	2013-01-01
H04L	/	2209	/	56	A	2013-01-01

CPC Combination Sets								
Symbol					Type	Set	Ranking	Version
	/		/					

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	18	
/JAMES D NIGH/ Senior Examiner, Art Unit 3685	07 October 2021	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

U.S. Patent and Trademark Office — Part of Paper No.: 20211006

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/309,612	Middleton et al.
	Examiner	Art Unit
	JAMES D NIGH	3685

INTERNATIONAL CLASSIFICATION					
CLAIMED					
H04L	/	9	/	32	

NON-CLAIMED					
	/		/		

US ORIGINAL CLASSIFICATION	
CLASS	SUBCLASS
705	64

CROSS REFERENCES(S)						
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)					

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	18	
/JAMES D NIGH/ Senior Examiner, Art Unit 3685	07 October 2021	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

U.S. Patent and Trademark Office — Part of Paper No.: 20211006

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/309,612	Middleton et al.
	Examiner	**Art Unit**
	JAMES D NIGH	3685

☑ 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	1		10		19	15	28								
	2		11	11	20	16	29								
2	3	7	12		21		30								
3	4		13		22	17	31								
4	5		14	12	23		32								
5	6	8	15	13	24	18	33								
	7	9	16		25										
	8	10	17	14	26										
6	9		18		27										

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	18	
/JAMES D NIGH/ Senior Examiner, Art Unit 3685	07 October 2021	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

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

86636 7590 10/19/2021
BRUNDIDGE & STANGER, P.C.
1925 BALLENGER AVENUE, STE. 560
ALEXANDRIA, VA 22314

EXAMINER
NIGH, JAMES D

ART UNIT	PAPER NUMBER
3685	

DATE MAILED: 10/19/2021

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/309,612	11/08/2016	Reginald Middleton	4675.1002BS	2321

TITLE OF INVENTION: Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers

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	01/19/2022

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)

86636 7590 10/19/2021
BRUNDIDGE & STANGER, P.C.
1925 BALLENGER AVENUE, STE. 560
ALEXANDRIA, VA 22314

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.
15/309,612	11/08/2016	Reginald Middleton	4675.1002BS	2321

TITLE OF INVENTION: Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers

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	01/19/2022

EXAMINER	ART UNIT	CLASS-SUBCLASS
NIGH, JAMES D	3685	705-064000

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.
15/309,612	11/08/2016	Reginald Middleton	4675.1002BS	2321

86636 7590 10/19/2021

BRUNDIDGE & STANGER, P.C.
1925 BALLENGER AVENUE, STE. 560
ALEXANDRIA, VA 22314

EXAMINER	
NIGH, JAMES D	
ART UNIT	PAPER NUMBER
3685	

DATE MAILED: 10/19/2021

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.** 15/309,612	**Applicant(s)** Middleton et al.	
	Examiner JAMES D NIGH	**Art Unit** 3685	**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 request for continued examination filed on July 27, 2021.
   ☐ 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 See Continuation Sheet . 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 _____.

/JAMES D NIGH/
Senior Examiner, Art Unit 3685

Continuation of 3. The allowed claim(s) is/are: 1,3-6,9,12,15-17,20,23-24,26,28-29,31 and 33

DETAILED ACTION

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.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on July 27, 2021 has been entered.

Claim Status

3. As of the Office Action dated January 27, 2021 claims 1, 3-6, 9, 12, 15-17, 20, 23-24, 26, 28-29 and 31-32 were pending and claims 1, 3-6, 9, 12, 15-17, 20, 23-24, 26, 28-29 and 31-32 stood rejected. Claims 1, 12, 24 and 28 have been amended. Claim 32 has been cancelled and claim 33 has been added. Claims 1, 3-6, 9, 12, 15-17, 20, 23-24, 26, 28-29, 31 and 33 are therefore currently pending and are presented for examination on the merits.

Response to Arguments

4. Applicant's argument with regard to the 35 U.S.C. § 101 rejection of claims 1, 3-6, 9, 12, 15-17, 20, 23-24, 26, 28-29 and 31-32 has been fully considered and is persuasive. Public key cryptography is present in the claim and the use of the private key to compute a cryptographic signature, while mathematical in nature, does not

encompass the types of operations performed by human beings prior to the invention of a programmed computer and Examiner now views these as not being abstract ideas. Furthermore the use of public key cryptography can be viewed as an additional element that forms a practical application of the abstract idea as clearly the claim is directed towards a payment transaction which does fall under the guidance with regard to certain methods of organizing human activity. As the claim is now deemed as being eligible under Prong Two of Step 2A the rejection is being withdrawn.

5. Applicant's argument with regard to the 35 U.S.C. § 112 (b) rejection of claims 12, 15-17, 23 and 32 has been fully considered and is persuasive. Accordingly the rejection is being withdrawn.

6. Applicant's argument with regard to the 35 U.S.C. § 103 rejection of claims 1, 3-6, 9, 12, 15-17, 20, 23, 24, 26, 28, 29, 31 and 32 as being unpatentable over Rosen (U.S. Patent Publication 2003/0070080) in view of Feigelson (U.S. Patent Publication 2013/0166455) in view of Ginter et al. (U.S. Patent Publication 2009/0030768, now U.S. Patent 7,587,369, hereinafter referred to as Ginter) has been fully considered and is persuasive. Examiner does view that those skilled in the art would at least consider prior art teachings regarding centralized systems in implementing a decentralized system and therefore are at least somewhat relevant to the processing of a financial transaction. Clearly Rosen provides advantages in the form cryptographically secure sessions and the exchanging of economic value both securely and reliably which is something that would likely draw the attention of those skilled in the art. Clearly however Rosen in the year 2003 could not have considered the use of cryptocurrency and a distributed ledger as it was taught by Feigelson ten years later. However this

would not end the obviousness inquiry as the inquiry centers on what one skilled in the art would have considered at the time of filing of the application which in this case would occur in the year 2014. However in further reviewing the Feigelson reference Examiner notes that the reference is directed towards the physical implementation of a digital currency and therefore Examiner must concede that even though Feigelson does teach the use of digital currency in the form of Bitcoin and at least by inference an inclusion of a distributed ledger no clear indication is present in Feigelson that Feigelson was concerned with anything other than making Bitcoin easier to spend by making it tangible. The two references produce an awkward combination in that regard and Examiner must concur with Applicant that combining Rosen and Feigelson requires hindsight reasoning in order to construct the rejection. Accordingly the rejection is being withdrawn.

Allowable Subject Matter

7. Claims 1, 3-6, 9, 12, 15-17, 20, 23-24, 26, 28-29, 31 and 33 are allowed.

8. The following is an examiner's statement of reasons for allowance:

9. Examiner has reconsidered the two prior art references and the combination of those references (Rosen and Feigelson) and concurs with Applicant that only through hindsight reasoning using the Applicant's disclosure for a roadmap would those of ordinary skill arrived at the combination of references and therefore the Examiner has reconsidered whether the previously issued rejection actually forms a prima facie case. In reviewing other prior art Examiner found other references that were indicative of related activity in the year of filing including Langschaedel et al. (U.S. Patent Publication 2015/0262171) which teaches the use and exchange of Bitcoin and has some indication

of using a data source for determining value of the digital currency (0101, 0135) but does not clearly include this as part of the transaction parameters as is claimed ("value data from at least one of the first data source or the second data source") and therefore does not alone or in combination teach this part of the claim. Examiner also reviewed Antonopoulos ("Mastering Bitcoin – Unlocking Digital Crypto-Currencies", O'Reilly Media, Inc., December, 2014) as on the second page of the electronic publication the page indicates that the work was copyrighted in the year 2010. However when Examiner went to the public site for the U.S. Copyright Office Examiner could only verify that a copyright was registered at the same time as publication of the printed publication and therefore Examiner could not conclusively establish that the book constituted prior art for purposes of patent examination. While it would appear that Antonopoulos would read on the claimed invention it does form the basis of a sustainable rejection under section 102. Therefore the claims are allowable over the prior art.

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

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JAMES D NIGH whose telephone number is (571)270-5486. The examiner can normally be reached 5 to 7:15 AM and 10:45 AM to 4:30 PM.

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, Neha Patel can be reached on (571) 270-1492. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of published or unpublished applications may be obtained from Patent Center. Unpublished application information in Patent Center is available to registered users. To file and manage patent submissions in Patent Center, visit: https://patentcenter.uspto.gov. Visit https://www.uspto.gov/patents/apply/patent-center for more information about Patent Center and https://www.uspto.gov/patents/docx for information about filing in DOCX format. For additional questions, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/JAMES D NIGH/
Senior Examiner, Art Unit 3685

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/309,612	Middleton et al.
	Examiner	Art Unit
	JAMES D NIGH	3685

CPC - Searched*		
Symbol	**Date**	**Examiner**
H04L 9/3247	01/22/2021	JDN
G06Q 20/02,065,10	01/22/2021	JDN
G06Q 40/02	01/22/2021	JDN
H04L 29/06	01/22/2021	JDN
H04L 2209/38,56	01/22/2021	JDN
H04L 9/3247	10/07/2021	JDN
G06Q 20/02,065,10	10/07/2021	JDN
G06Q 40/02	10/07/2021	JDN
H04L 29/06	10/07/2021	JDN
H04L 2209/38,56	10/07/2021	JDN

CPC Combination Sets - Searched*		
Symbol	**Date**	**Examiner**

US Classification - Searched*			
Class	**Subclass**	**Date**	**Examiner**
705	64	10/07/2021	JDN

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

	/JAMES D NIGH/ Senior Examiner, Art Unit 3685

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/309,612	Middleton et al.
	Examiner	Art Unit
	JAMES D NIGH	3685

Search Notes		
Search Notes	**Date**	**Examiner**
EAST Text Search	07/18/2019	JDN
EAST Text Search	06/05/2020	JDN
PE2E Text and Classification Search	01/22/2021	JDN
PE2E Text, Classification and inventor search	10/07/2021	JDN
IP.Com Patent and NPL Search	10/07/2021	JDN
Dialog ProQuest NPL Search	10/07/2021	JDN
Google Search	10/07/2021	JDN
Google Scholar Search	10/07/2021	JDN

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**
705	64	10/07/2021	JDN

	/JAMES D NIGH/ Senior Examiner, Art Unit 3685

Concurrency in **Blockchain Based** Smartpool with Transactional Memory

L Kadariya - 2018 - search.proquest.com

... , wallet creates the transaction from the **UXTO**, **digitally** signs the transaction and send it to ... As UTXO refers to output of previous transaction, this **unspent** output(UTXO) may be larger than ... It is a **distributed ledger** technology which makes Bitcoin as a decentralized system. It is a ...

☆ 99 Related articles All 2 versions

The economics of **digital currencies**

P Ali, J Barrdear, R Clews... - Bank of England Quarterly ... , 2014 - papers.ssrn.com
... is the introduction of a '**distributed ledger**', which allows a **digital currency** to be used in a ... , miners must devote computing resources to **mathematical** puzzles that are hard to solve, but the ... As of 9 July 2014, there were almost 41 million addresses listed on the Bitcoin **block chain**, ...
☆ 99 Cited by 342 Related articles All 5 versions »

Mastering Bitcoin: unlocking **digital** cryptocurrencies

AM Antonopoulos - 2014 - books.google.com
... system, which operates **based** on fully transparent **mathematical** principles. The invention ... is finally recorded on the **block-chain**, the **distributed ledger** of all transactions. Each example is ... network and **block-chain**, we will use a **blockchain** explorer site to visualize each step. A ...
☆ 99 Cited by 1843 Related articles All 9 versions »

Bitcoin financial regulation: Securities, derivatives, prediction markets, and gambling

J Brito, H Shadab, A Castillo - Colum. Sci. & Tech. L. Rev., 2014 - HeinOnline
... Additionally, the **block chain** technology that Bitcoin introduced for the first time makes ... properties allow it to simultaneously serve as a **currency** and a **distributed ledger** system. ... The **mathematical** relationship between a given public key and the corresponding private key allows ...
☆ 99 Cited by 178 Related articles All 9 versions

The value of Bitcoin in enhancing the efficiency of an investor's portfolio

CY Wu, VK Pandey, C Dba - Journal of ..., 2014 - financialplanningassociation.org
... the function of maintaining the **block chain**, a public and **distributed ledger**, to keep track of ... increasingly complicated **mathematical** problems that verify transactions in the **block chain** so ... **blockchain**.info, in 2013 the number of daily transactions has only once exceeded 100,000. ...
☆ 99 Cited by 120 Related articles All 3 versions »

Bitcoin and other **virtual currencies** for the 21st century

JA Malone - 2014 - books.google.com
... Every bitcoin transaction is registered in this public, **distributed ledger**, or **block chain**. The **blockchain** public ledger is the heart of the Bitcoin ... are created or "mined" as thousands of dispersed computers solve complex **math** problems that verify the transactions in the **block chain**. ...
☆ 99 Cited by 5 Related articles All 2 versions »

Virtually possible: how to strengthen Bitcoin regulation within the current regulatory framework

P Kirby - NCL Rev., 2014 - HeinOnline
... / ("Bitcoin is an Internet-wide **distributed ledger**. You buy into the ledger by purchasing one of ... by default, visible to anyone who searches the **blockchain**, the distributed public ledger of all [... **math** problems, which in turn verify the transactions in the public key ledger, or **block chain**....
☆ 99 Cited by 16 Related articles All 5 versions

Bitcoin-The Political'**Virtual**'of an Intangible Material **Currency**.

MA Jansen - 2012 - dspace.library.uu.nl

... 18 The **block chain** is what enables Bitcoin to solve the 'double-spending problem', that is ... Bitcoin's **blockchain** acts as a clearinghouse, but one where all users participate and sign off ... 20 Given that the difficulty of the **mathematical** problems increases over time, solving them ...

☆ 99 Cited by 19 Related articles All 2 versions »

Getting started with Bitcoins

J Stevenson - 2013 - books.google.com

... Instead, it uses a **distributed ledger** book system (called a "**blockchain**") **based** on the logic ... When you perform mining, your computer adds new Bitcoin transactions to the **block chain** (... making it ideal for ripping through the **currency's** core **mathematical** algorithm. But think twice if ...

☆ 99 Cited by 4 Related articles »

Bitcoins, litecoins, what coins?: A global phenomenon

J Stevenson - 2013 - books.google.com

... eliminate trackable linkage in the Bitcoin **blockchain**, which would make Bitcoin anonymous ... In the Ripple model, gateways issue balances onto Ripple's **distributed ledger**. In this way, ... **block chain**. The process of finding these hashes and creating blocks is called mining). 45 ...

☆ 99 Cited by 4 Related articles »

BitProperty

JAT Fairfield - S. Cal. L. Rev., 2014 - HeinOnline

... The term "**block chain**" can refer either to the Bitcoin **block chain**, or to the **block chain** ... who implement the protocol, or the essential **mathematical** soundness of the protocol itself in the face ... Thus, for example, in May 2013, the founder and operators of **electronic currency** system ...

☆ 99 Cited by 132 Related articles All 4 versions

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L1	5	("20030070080"|"20130054471"|"20130166455"|"20130179337"|"20130212388").PN.	(US-PGPUB; USPAT)	AND	ON	ON	2019/07/18 07:53 AM
L2	17	(server near20 ("public key") near20 ("private key")) ((transaction or principal) near10 amount) (signature near20 "private key") ((client or agent) near20 "private key") ((digital or electronic) near10 currency) @ad<="20140509"	(US-PGPUB; USPAT)	AND	ON	ON	2019/07/18 08:22 AM
L3	2	("20170187535").PN.	(US-PGPUB; USPAT; USOCR; DERWENT)	AND	ON	ON	2019/12/09 12:05 PM
L4	17	((intermediary OR server) near20 ("public key") near20 ("private key")) ((transaction or principal) near10 amount) (signature near20 "private key") ((client or agent) near20 "private key") ((digital or electronic) near10 currency) @ad<="20140509"	(US-PGPUB; USPAT)	AND	ON	ON	2020/06/01 12:40 PM
L5	17	((intermediary OR server) near20 ("public key") near20 ("private key")) ((transaction or principal) near10 amount) (signature near20 "private key") ((client or agent) near20 "private key") ((digital or electronic) near10 currency) (@ad<="20140509" OR @pd<="20140509" @rlad<="20140509" OR @prad<="20140509") NOT ("continuation-in-part" AND @ad>"20140509")	(US-PGPUB; USPAT)	AND	ON	ON	2020/06/01 12:41 PM
L6	2	((US-20130166455-A1 OR US-20030070080-A1).did. AND	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO, JP, EP, KR);	AND	ON	ON	2020/09/15 12:31 PM

		PGPB.dbnm.)	FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L7	69006	(@ad<=20140509 OR @pd<=20140509 OR @rlad<=20140509 OR @prad<=20140509) NOT ("continuation-in-part" AND @ad>20140509) oracle	(US-PGPUB; USPAT)	AND	ON	ON	2021/01/19 11:51 AM
L8	5	(@ad<=20140509 OR @pd<=20140509 OR @rlad<=20140509 OR @prad<=20140509) NOT ("continuation-in-part" AND @ad>20140509) (oracle near20 transaction near20 event)	(US-PGPUB; USPAT)	AND	ON	ON	2021/01/19 11:52 AM
L9	123593	(@ad<=20140509 OR @pd<=20140509 OR @rlad<=20140509 OR @prad<=20140509) NOT ("continuation-in-part" AND @ad>20140509) (external near5 (state OR event))	(US-PGPUB; USPAT)	AND	ON	ON	2021/01/19 11:53 AM
L10	158	(@ad<=20140509 OR @pd<=20140509 OR @rlad<=20140509 OR @prad<=20140509) NOT ("continuation-in-part" AND @ad>20140509) (external near5 (state OR event)) (asset near5 transaction)	(US-PGPUB; USPAT)	AND	ON	ON	2021/01/19 11:54 AM
L11	9104	(@ad<=20140509 OR @pd<=20140509 OR @rlad<=20140509 OR @prad<=20140509) NOT ("continuation-in-part" AND @ad>20140509) ("multi-sig" OR (multiple near3 signature))	(US-PGPUB; USPAT)	AND	ON	ON	2021/01/19 12:50 PM
L12	141	(@ad<=20140509 OR @pd<=20140509 OR @rlad<=20140509 OR @prad<=20140509) NOT ("continuation-in-part" AND @ad>20140509) (("multi-sig" OR (multiple near3	(US-PGPUB; USPAT)	AND	ON	ON	2021/01/19 12:50 PM

		signature)) near20 transaction)					
L13	263	(@ad<=20140509 OR @pd<=20140509 OR @rlad<=20140509 OR @prad<=20140509) NOT ("continuation-in-part" AND @ad>20140509) (("multi-sig" OR (multiple near3 signature)) near20 transaction)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2021/01/19 02:55 PM
L14	1	(@ad<=20140509 OR @pd<=20140509 OR @rlad<=20140509 OR @prad<=20140509) NOT ("continuation-in-part" AND @ad>20140509) (("multi-sig" OR (multiple near3 signature)) near20 transaction) oracle	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2021/01/19 02:55 PM
L15	152	(@ad<=20140509 OR @pd<=20140509 OR @rlad<=20140509 OR @prad<=20140509) NOT ("continuation-in-part" AND @ad>20140509) (notariz$4 near5 transaction)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2021/01/20 07:24 AM
L16	76	(@ad<=20140509 OR @pd<=20140509 OR @rlad<=20140509 OR @prad<=20140509) NOT ("continuation-in-part" AND @ad>20140509) (notariz$4 near5 transaction) contract	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2021/01/20 08:21 AM
L17	14	(@ad<=20140509 OR @pd<=20140509 OR @rlad<=20140509 OR @prad<=20140509) NOT ("continuation-in-part" AND @ad>20140509) (notariz$4 near5 transaction) contract fulfill$5	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2021/01/20 08:21 AM
L18	7	(@ad<=20140509 OR @pd<=20140509 OR @rlad<=20140509 OR @prad<=20140509)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR,	AND	ON	ON	2021/01/21 07:46 AM

		NOT ("continuation-in-part" AND @ad>20140509) (notariz$4 near5 transaction) contract fulfill$5 (H04L9/3247 OR G06Q20/065 OR G06Q40/02 OR H04L29/06 OR G06Q20/02 OR G06Q20/10 OR H04L2209/38 OR H04L2209/56).cpc.	GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)				
L19	7	((US-20130166455-A1 OR US-20030070080-A1 OR US-20150287026-A1 OR US-20090025087-A1 OR US-20090030768-A1).did. AND PGPB.dbnm.) OR ((US-20100138659-A1).did. AND DWPI.dbnm.) OR ((US-7587369-B2).did. AND USPT.dbnm.)	(USPAT; US-PGPUB; FPRS; USOCR; IBM_TDB; EPO; JPO; DERWENT; FIT (AU, AP, AT, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO))	AND	ON	ON	2021/01/21 07:46 AM
L21	2	(@ad<=20140509 OR @pd<=20140509 OR @rlad<=20140509 OR @prad<=20140509) NOT ("continuation-in-part" AND @ad>20140509) (notariz$4 near5 transaction) contract fulfill$5 untrusted	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2021/01/22 10:50 AM
L22	5	(@ad<=20140509 OR @pd<=20140509 OR @rlad<=20140509 OR @prad<=20140509) NOT ("continuation-in-part" AND @ad>20140509) (notariz$4 near5 transaction) contract untrusted	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2021/01/22 10:50 AM
L23	17525	(@ad<="20140509" OR @pd<="20140509" OR @rlad<="20140509" OR @prad<="20140509") NOT ("continuation-in-part" AND @ad>"20140509") (blockchain OR "block chain" OR "distributed ledger")	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2021/10/05 01:10 PM

L24	62	(@ad<="20140509" OR @pd<="20140509" OR @rlad<="20140509" OR @prad<="20140509") NOT ("continuation-in-part" AND @ad>"20140509") (blockchain OR "block chain" OR "distributed ledger") ((digital OR electronic) near5 currency)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2021/10/05 01:10 PM
L25	76	(@ad<="20140509" OR @pd<="20140509" OR @rlad<="20140509" OR @prad<="20140509") NOT ("continuation-in-part" AND @ad>"20140509") (blockchain OR "block chain" OR "distributed ledger") ((virtual OR (math near3 based) OR digital OR electronic) near5 currency)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2021/10/05 01:52 PM
L26	77	(@ad<="20140509" OR @pd<="20140509" OR @rlad<="20140509" OR @prad<="20140509") NOT ("continuation-in-part" AND @ad>"20140509") (blockchain OR "block chain" OR "distributed ledger") ((virtual OR (math near3 based) OR digital OR electronic) near5 currency)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2021/10/05 01:59 PM
L27	11	(@ad<="20140509" OR @pd<="20140509" OR @rlad<="20140509" OR @prad<="20140509") NOT ("continuation-in-part" AND @ad>"20140509") (blockchain OR "block chain" OR "distributed ledger") ((virtual OR (math near3 based) OR digital OR electronic) near5 currency)	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO;	AND	ON	ON	2021/10/05 02:11 PM

		(commit$) (unspent OR uxto)	JPO; DERWENT; IBM_TDB)				
L28	16	"660331".ap.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, MC, MD, MY, NL, NO, NZ, OA, PH, PL, PT, RO, RS, RU, SE, SG, SI, SK, SU, TH, TN, TR, TW, UA, VN, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2021/10/07 03:36 PM
L29	8	((US-20130166455-A1 OR US-20030070080-A1 OR US-20150287026-A1 OR US-20090025087-A1 OR US-20090030768-A1 OR US-20150262171-A1).did. AND PGPB.dbnm.) OR ((US-20100138659-A1).did. AND DWPI.dbnm.) OR ((US-7587369-B2).did. AND USPT.dbnm.)	(USPAT; US-PGPUB; FPRS; USOCR; IBM_TDB; EPO; JPO; DERWENT; FIT (AU, AP, AT, BE, BG, BR, BY, CA, CH, CN, CS, CU, CZ, DD, DE, DK, EA, EE, EP, ES, FI, FR, GB, HR, HU, ID, IE, IL, IS, IT, JP, KR, LT, LU, LV, MA, OA, RU, SU, WO, MC, MD, MY, NL, NO, NZ, PH, PL, PT, RO, RS, SE, SG, SI, SK, TH, TN, TR, TW, UA, VN))	AND	ON	ON	2021/10/07 03:38 PM
L30	0	(@ad<="20140509" OR @pd<="20140509" OR @rlad<="20140509" OR @prad<="20140509") NOT ("continuation-in-part" AND @ad>"20140509") (notariz$4 near5 transaction) contract fulfill$5 705/64.ccls.	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	AND	ON	ON	2021/10/07 04:06 PM
L31	53	("2015/0262171").urpn. AND (PGPB | USPT | USOC).dbnm.	(US-PGPUB; USPAT; USOCR)	AND	ON	ON	2021/10/07 04:08 PM
L32	186	("4790431" | "5799287" | "5950176" | "6021257" | "6157920" | "6505174" | "6523012" | "6583712" | "7391865" | "7487123" | "7677974" | "7716484" | "7870058" | "8108278" | "8108283" | "8224702"	(US-PGPUB; USPAT; USOCR)	AND	ON	ON	2021/10/07 04:10 PM

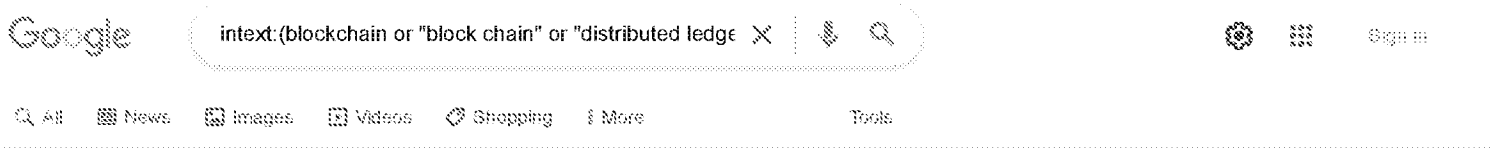
		| "8229855" | "8229859" | "8239330" | "8255297" | "8275692" | "8306910" | "8326751" | "8352326" | "8452703" | "8606685" | "8630951" | "8688525" | "8688563" | "8712914" | "8719131" | "9794074" | "20020143614" | "20020171546" | "20030009413" | "20030014749" | "20030225672" | "20040049464" | "20040143710" | "20040193657" | "20040243488" | "20050044022" | "20070117615" | "20070146797" | "20070219869" | "20070271455" | "20080109280" | "20080120221" | "20080140578" | "20080167965" | "20080215474" | "20080243703" | "20080249957" | "20080281444" | "20090089168" | "20090094134" | "20090098939" | "20090119200" | "20090132830" | "20090265268" | "20100174646" | "20100228674" | "20100250360" | "20100306084" | "20110110516" | "20110112662" | "20110231913" | "20110270748" | "20120078693" | "20120101886" | "20120123924" | "20120185395" | "20120239543" | "20120278200" | "20130036373" | "20130041773" | "20130054471" | "20130061049" | "20130159699" | "20130166455" | "20130191277" | "20130232023" |					

		"20130238478" | "20130246233" | "20130254052" | "20130311266" | "20130311348" | "20130317972" | "20130317984" | "20130325701" | "20140025473" | "20140032267" | "20140040157" | "20140081710" | "20140122903" | "20140141869" | "20140156497" | "20140164251" | "20140233740" | "20140280476" | "20140310527" | "20140344015" | "20150033301" | "20150120567" | "20150120569" | "20150170112" | "20150193744" | "20150227897" | "20150244690" | "20150262137" | "20150262138" | "20150262139" | "20150262140" | "20150262141" | "20150262168" | "20150262171" | "20150262172" | "20150262173" | "20150262176" | "20150310424" | "20150324787" | "20150332283" | "20150341422" | "20150348169" | "20150356523" | "20150356555" | "20150363777" | "20150363783" | "20150379510" | "20160027229" | "20160028552" | "20160078219" | "20160080156" | "20160086187" | "20160092988" | "20160112200" | "20160125040" | "20160162873" | "20160203448" | "20170005804" |				

		"20170017955" | "20170091750" | "20170124535" | "20170132630").pn. OR ("9892460").urpn. AND (PGPB | USPT | USOC).dbnm.					
L33	129	32 (@ad<="20140509" OR @pd<="20140509" OR @rlad<="20140509" OR @prad<="20140509") NOT ("continuation-in-part" AND @ad>"20140509")	(US-PGPUB; USPAT)	AND	ON	ON	2021/10/07 04:11 PM
L34	24	32 (@ad<="20140509" OR @pd<="20140509" OR @rlad<="20140509" OR @prad<="20140509") NOT ("continuation-in-part" AND @ad>"20140509") (blockchain OR "block chain" OR "distributed ledger")	(US-PGPUB; USPAT)	AND	ON	ON	2021/10/07 04:11 PM
L35	12	((("MIDDLETON") near3 ("Reginald")) OR (("BOGOSIAN") near3 ("Matthew"))).INV.	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	AND	ON	ON	2021/10/07 04:17 PM

PE2E SEARCH - Search History (Interference)

There are no Interference searches to show.



About 2 results (0.51 seconds)

Did you mean: intext:(blockchain or "block chain" or "distributed ledger") AND intext:((virtual or (math AROUND(3) based) or digital or electronic) AROUND(5) currency) AND intext:(commit*) AND intext:(unspent or *utxo*) AND intext:(timestamp or "time stamp") AND intext:lock*

It looks like there aren't many great matches for your search

Tip: Try using words that might appear on the page you're looking for. For example, "cake recipes" instead of "how to make a cake."

Need help? Check out other tips for searching on Google.

You can also try this search:

blockchain is the digital distributed and decentralized ledger underlying most virtual currencies

https://ebin.pub › electronic-trading-and-blockchain-ye...

Electronic Trading and Blockchain: Yesterday, Today and ...

Digital or virtual seems to be used interchangeably as describing currencies based on an electronic medium. However, they are not synonyms.

http://80.87.201.18 › text › blockchain glossary of terms

["The goal of this technology is to automate events and reduce the ...

The blockchain, for example, is a distributed ledger that was originally created to keep track of all bitcoin transactions.","As these new blocks are ...

People also search for

what's blockchain blockchain bitcoin

Ad · https://bootcamp.uncc.edu/blockchain/apply_today

Become a Blockchain Developer - UNC Charlotte

Learn to use Solidity, Consensus Algorithms, Ganache & more to advance your career. Gain real-world experience with the tools you need to succeed in the FinTech industry.
Early Registration Prices · Part-Time Course · Career Services · Apply Now

Ad · https://emeritus.gsb.columbia.edu/columbia/blockchain

Learn the Basics of Blockchain - Columbia Executive Education

Examine the opportunities and challenges of **Blockchain** and Cryptocurrencies. Apply now! Discover how **Blockchain** can change business for the better in this online program. Flexible Payment Options. 2-month Online Program. 4-6 Hours per Week. Starts Nov 9, 2021.
Blockchain Technology · Program Highlights · Key Takeaways · Enroll Now

Ad · https://mit-online.getsmarter.com/mit-blockchain/online-course (617) 997-4979

MIT Sloan Blockchain Program - 6-Week Online Short Course

Study **Blockchain** Technologies in Business Innovation Application. Learn More Today! Earn Your Certificate of Completion from the MIT Sloan School of Management. Flexible Learning. Structured Approach. Weekly Modules. Top-Tier University. Personalized Support.

Related searches

what's blockchain blockchain bitcoin

28374, North Carolina - Based on your past activity - Update location

Help Send feedback Privacy Terms

Search History 15309612

Report Run Date: 2021-10-06 UTC
Queries: 4
Markers: 0

Query #	Timestamp	Results	Page
1	2021-10-06 11:12 UTC	2,664,156	3
2	2021-10-06 11:18 UTC	2	3
3	2021-10-06 11:33 UTC	14,777,115	4
4	2021-10-06 11:34 UTC	7	4

Content: Non-Patent Literature (23)

IEEE Xplore Publications: IEEE Periodicals | IEEE Xplore Publications: IEEE Conferences | IEEE Xplore Publications: IEEE Standards | IEEE Xplore Publications: IEEE Early Access | 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 | Other Literature: IBM Redbooks | Other Literature: PubMed Central | Other Literature: arXiv.org

1 **2021-10-06 11:12 UTC | 2,664,156 results from**

De-Dup: None | **Cut-off:** None | **Sort:** Relevance

Main Concept: Document
US20170187535 Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers (view)

Concept Modifiers: None

Filters: None

2 **2021-10-06 11:18 UTC | 2 results from**

De-Dup: None | **Cut-off:** None | **Sort:** Relevance

Main Concept: Same as Query 1

Concept Modifiers: None

Filters (2):
Publication Date: From 1980-01-01 To 2014-05-09
Classic Syntax limited to: (blockchain OR "block chain" OR "distributed ledger") ((virtual OR (math near3 based) OR digital OR electronic) near5 currency) (commit*) (unspent OR uxto)

Content: Patent Publications (164)

US Patents | US Designs | US Applications | EPO Patents | EPO Applications | China Patents | China Applications | Japan Patents | Japan Applications | Korea Patents | Korea Applications | WIPO Applications | Argentina Patents | Argentina Applications | Brazil Patents | Brazil Applications | Canada Patents | Canada Applications | Chile Patents | Chile Applications | Colombia Applications | Costa Rica Applications | Cuba Patents | Cuba Applications | Dominican Republic Applications | Ecuador Patents | Ecuador Applications | El Salvador Applications | Guatemala Applications | Honduras Applications | Mexico Patents | Mexico Applications | Nicaragua Patents | Panama Applications | Peru Applications | Trinidad & Tobago Patents | Uruguay Applications | Austria Patents | Austria Applications | Belarus Patents | Belgium Patents | Belgium Applications | Bosnia & Herzegovina Patents | Bosnia & Herzegovina Applications | Bulgaria Patents | Bulgaria Applications | Croatia Patents | Croatia Applications | Czech Republic Patents | Czech Republic Applications | Czechoslovakia Patents | Czechoslovakia Applications | Denmark Patents | Denmark Applications | Estonia Patents | Estonia Applications | EUIPO Patents | Finland Patents | Finland Applications | France Patents | France Applications | Germany Patents | Germany Applications | Great Britain Patents | Great Britain Applications | Greece Patents | Greece

Applications | Hungary Patents | Hungary Applications | Iceland Patents | Iceland Applications | Ireland Patents | Ireland Applications | Italy Patents | Italy Applications | Latvia Patents | Latvia Applications | Lithuania Patents | Lithuania Applications | Luxembourg Patents | Malta Patents | Monaco Patents | Montenegro Patents | Montenegro Applications | Netherlands Patents | Netherlands Applications | Norway Patents | Norway Applications | Poland Patents | Poland Applications | Portugal Patents | Portugal Applications | Republic of Moldova Patents | Republic of Moldova Applications | Romania Patents | Romania Applications | San Marino Patents | San Marino Applications | Serbia Patents | Serbia Applications | Slovakia Patents | Slovakia Applications | Slovenia Patents | Spain Patents | Spain Applications | Sweden Patents | Sweden Applications | Switzerland Patents | Switzerland Applications | Ukraine Patents | Yugoslavia/Serbia and Montenegro Patents | Yugoslavia/Serbia and Montenegro Applications | Armenia Patents | Australia Patents | Australia Applications | Cyprus Patents | Gulf Cooperation Council Patents | Hong Kong Patents | India Patents | India Applications | Indonesia Patents | Indonesia Applications | Israel Applications | Jordan Patents | Kyrgyzstan Patents | Macao Applications | Malaysia Patents | Mongolia Patents | New Zealand Patents | Philippines Patents | Philippines Applications | Saudi Arabia Patents | Singapore Patents | Singapore Applications | Taiwan Patents | Taiwan Applications | Tajikistan Patents | Tajikistan Applications | Thailand Applications | Uzbekistan Patents | Vietnam Patents | Algeria Patents | ARIPO Patents | ARIPO Applications | Egypt Patents | Kenya Patents | Malawi Patents | Morocco Patents | Morocco Applications | OAPI Patents | South Africa Patents | Tunisia Applications | Zambia Patents | Zimbabwe Patents | EAPO Patents | EAPO Applications | Georgia Patents | Georgia Applications | Kazakhstan Patents | Kazakhstan Applications | Russia Patents | Russia Applications | Turkey Patents | Turkey Applications

3 **2021-10-06 11:33 UTC | 14,777,115 results from**

De-Dup: None | **Cut-off:** None | **Sort:** Relevance

Main Concept: Document
US20170187535 Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers (view)

Concept Modifiers: None

Filters: None

4 **2021-10-06 11:34 UTC | 7 results from**

De-Dup: None | **Cut-off:** None | **Sort:** Relevance

Main Concept: Same as Query 3

Concept Modifiers: None

Filters (2):
Classic Syntax limited to: (blockchain OR "block chain" OR "distributed ledger") ((virtual OR (math near3 based) OR digital OR electronic) near5 currency) (commit*) (unspent OR uxto)
Earliest Priority Date: From 1980-01-01 To 2014-05-09

The **ClinicalTrials.gov** full text database is now available.

Dialog

ProSheets | Account | Help | Workspace

Basic Search | Advanced | Command Line | Find Similar | Look Up Citation | 1 Recent searches | 0 Selected items

Your search for *(blockchain or "block chain" or "distributed ledger") and ((virtual or (math near/3 based) or digital or electronic) near/5 currency) and (commit*) and (unspent or uxto) and (timestamp or "time stamp") and lock** found 0 results.

Please modify your search and try again. Search tips

Add search fields | Thesaurus | Look up terms | Field Codes | Search tips | Help | Search Translator

Translate BRS to Dialog search syntax. The translation is limited to internal EAST settings.

BRS EAST search syntax | Translate | Dialog search syntax | Align sets

(blockchain OR "block chain" OR "distributed ledger") and ((virtual OR (math near3 based) OR digital OR electronic) near5 currency) and (commit$) and (unspent OR uxto) and (timestamp OR "time stamp") and lock*

(blockchain or "block chain" or "distributed ledger") and ((virtual or (math near/3 based) or digital or electronic) near/5 currency) and (commit*) and (unspent or uxto) and (timestamp or "time stamp") and lock*

Enter your search set(s), e.g., TI(nursing) and AU(smith).

Start each set on a new line using **Enter** or **Shift+Enter**.

Preview result counts | Search | Clear form

nurs* finds up to 10 characters (e.g., nurse, nurses, nursing) with unlimited word variations. Learn more

Limit to: ☐ Full text ☐ Peer reviewed

Publication date: Specific date range...

Search for a range of years, years and months, or specific dates

Start

January | 1 | 1980 (yyyy)

DialogSolutions

Literature · Technology · Services

Copyright 2021 ProQuest LLC. All rights reserved.

Sort results by: Relevance

Items per page: 20

Duplicates: Include duplicate documents

Preview result counts | Search | Clear form

DialogSolutions
Literature · Technology · Services

Contact Us Privacy Policy Cookie Preferences Accessibility Sitemap
Terms and Conditions

Copyright 2021 ProQuest LLC. All rights reserved.

Copyright

The Library has opened access to the reading rooms by appointment only. More. The Jefferson Building has reopened to visitors via timed, ticketed entry. More.

Help | Search | History | Titles | Start Over

Public Catalog

Copyright Catalog (1978 to present)
Search Request: Left Anchored Title = mastering bitcoin
Search Results: Displaying 1 through 3 of 3 entries.

previous next

Resort results by:

Set Search Limits

#	Title <	Full Title	Copyright Number	Date
[1]	Mastering bitcoin.	Mastering bitcoin.	V9921D040	2015
[2]	Mastering Bitcoin.	Mastering Bitcoin.	TX0008000404	2014
[3]	Mastering Bitcoin, 2E.	Mastering Bitcoin, 2E.	TX0008458173	2017

Resort results by:

Set Search Limits

Clear Selected Retain Selected

previous next

Save, Print and Email (Help Page)

Records Select Format: Full Record Format for Print/Save

All on Page
Selected On Page
Selected all Pages

Enter your email address: Email

Search for: mastering bitcoin Search by: Title (omit initial article A, An, The, El, La, Das etc.) Item type: None

25 records per page Submit Reset

Help Search History **Titles** Start Over

Contact Us | Request Copies | Get a Search Estimate | Frequently Asked Questions (FAQs) about Copyright | Copyright Office Home Page | Library of Congress Home Page

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)

86636 7590 10/19/2021
BRUNDIDGE & STANGER, P.C.
1925 BALLENGER AVENUE, STE. 560
ALEXANDRIA, VA 22314

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.
15/309,612	11/08/2016	Reginald Middleton	4675.1002BS	2321

TITLE OF INVENTION: Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers

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	01/19/2022

EXAMINER	ART UNIT	CLASS-SUBCLASS
NIGH, JAMES D	3685	705-064000

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 BRUNDIDGE & STANGER, 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	(B) RESIDENCE: (CITY and STATE OR COUNTRY)
Reginald Middleton	Brooklyn, NY (USA)

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. 504888

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 /Misung Lee/ Date October 29, 2021

Typed or printed name Misung Lee Registration No. 78307

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
15/309,612	**10/29/2021 11:15:16 AM ET**	**4675.1002BS**

Title of Invention

Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers

Application Information

APPLICATION TYPE	Utility - U.S. National Stage under 35 USC 371	PATENT #	-
CONFIRMATION #	2321	FILED BY	Juel Clyne
PATENT CENTER #	60375782	FILING DATE	11/08/2016
CUSTOMER #	86636	FIRST NAMED INVENTOR	Reginald Middleton
INTL. APPLICATION #	-	INTL. FILING DATE	-
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Misung Lee

Documents

TOTAL DOCUMENTS: 1

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
IFTransmittal.pdf	1	Issue Fee Payment (PTO-85B)	196 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
IFTransmittal.pdf	E75B4C71EABCA6882439135F2AFE343DCD38F6A809DCC4D1 FCABE204BE216A1A0C1DF8327576EDB71AD0E4B49C922EB8 86D28E1EB38D52BAD3A2AB3155E6E3B1

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 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

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
15/309,612	10/29/2021 11:15:16 AM ET	4675.1002BS

Title of Invention

Devices, Systems, and Methods for Facilitating Low Trust and Zero Trust Value Transfers

Application Information

APPLICATION TYPE	Utility - U.S. National Stage under 35 USC 371	PATENT #	-
CONFIRMATION #	2321	FILED BY	Juel Clyne
PATENT CENTER #	60375782	AUTHORIZED BY	Misung Lee
CUSTOMER #	86636	FILING DATE	11/08/2016
INTL. APPLICATION #	-	INTL. FILING DATE	-
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	Reginald Middleton

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
CARD / 2003	E20210SB15540953	Juel Clyne

FEE CODE	DESCRIPTION	ITEM PRICE($)	QUANTITY	ITEM TOTAL($)
2501	UTILITY ISSUE FEE	600.00	1	600.00
			TOTAL AMOUNT:	$600.00

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 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.
15/309,612	12/07/2021	11196566	4675.1002BS	2321

86636 7590 11/17/2021

BRUNDIDGE & STANGER, P.C.
1925 BALLENGER AVENUE, STE. 560
ALEXANDRIA, VA 22314

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 550 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):

Reginald Middleton, Brooklyn, NY;

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.

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the District of Delaware on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT for the District of Delaware
PLAINTIFF Veritaseum Capital, LLC		DEFENDANT Coinbase Global, Inc.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	US 11,196,566 B2	12/7/2021	Reginald Middleton
2			
3			
4			
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**