



Australian Government

PCT/AU2016/000279

**Patent Office
Canberra**

I, VIVIENNE IGLESIAS, DELEGATE OF THE COMMISSIONER, hereby certify that annexed is a true copy of the Provisional specification in connection with Application No. 2016900239 for a patent by SPARRO (AUSTRALIA) PTY LTD as filed on 27 January 2016.

**WITNESS my hand this
THIRTEENTH day of September 2016**

**VIVIENNE IGLESIAS
DELEGATE OF THE COMMISSIONER**



Payment Messaging System

TECHNICAL FIELD

[0001] The present invention relates to settlement systems and, more particularly although not exclusively, to a payment messaging system particularly, although not exclusively, suited to electronic transactions.

BACKGROUND

[0002] "Settlement" in the sense of settling amounts owing as between two parties, whether in a Fiat currency or in the newer forms of electronic currency (such as "Bitcoin") is a known concept which is central to the workings of most financial systems. In the case of electronic currency which requires settlement by exchange of data between institutions the current system is quite cumbersome and leads to many costs due in part to the necessity for often repeated data entry of significant amounts of data into systems run by the parties to any given transaction requiring settlement and also to the intermediaries that in almost every instance (barring a non-electronic cash transaction) form part of a chain of intermediaries that become involved in ultimately effecting settlement of any given transaction.

[0003] In particular implementations of settlement systems across the internet, a blockchain structure may be utilised where a blockchain is a distributed database that maintains a continuously growing list of data records that may be hardened against tampering and revision. The most widely known application of a blockchain is the public ledger of transactions for cryptocurrencies, such as Bitcoin referenced above.

[0004] Many settlement systems are characterised by effectively one-way transmission of data in any given data exchange transaction (for example systems based on Swift messaging). If it is subsequently discovered that there are deficiencies in the data thus transmitted there can then ensue time consuming checking and querying operations before settlement can be effected.

[0005] It is an object of the present invention to address or at least ameliorate some of the above disadvantages.

Notes

[0006] The term “comprising” (and grammatical variations thereof) is used in this specification in the inclusive sense of “having” or “including”, and not in the exclusive sense of “consisting only of”.

[0007] The above discussion of the prior art in the Background of the invention, is not an admission that any information discussed therein is citable prior art or part of the common general knowledge of persons skilled in the art in any country.

SUMMARY OF INVENTION**Definitions:**

[0008] **token:** in this specification a "token" is a data record containing data required to settle a transaction for which the token has been generated; and wherein the data is rendered, formatted or passed through an algorithm in a predetermined manner. The process of rendering, formatting or passing through an algorithm in a predetermined manner is termed “tokenisation”. The tokenisation process may involve operations such as encryption and de-identification of data.

[0009] **Transaction:** in this specification "transaction" refers to a trade between two parties, for example at least a first transacting entity and a second transacting entity and wherein the trade is expressed in a financial form (for example in a Fiat currency or an electronic currency-to be distinguished, for example, from a barter transaction) which will ultimately require exchange of currency to settle the transaction. In some instances the currency will be the same on both sides of the transaction. In other cases a conversion from one currency to another may be required.

[00010] Accordingly, in one broad form of the invention, there is provided a system for settling a transaction electronically; said system comprising:

at least a first transacting entity;

at least a second transacting entity;

at least a first intermediary entity;

at least a second intermediary entity;

in the case where the first transacting entity enters into a transaction with the second transacting entity generating a tokenised message at the time of the transaction containing data needed to settle the transaction;
initiating settlement of the transaction by transmission of the tokenised message to the at least first transacting entity.

[00011] In a further broad form of the invention there is provided a tokenised message construction system; said system comprising:
a server in communication with a database and which facilitates communications between a plurality of parties to a transaction;
each party having a digitised device with which to communicate with other ones of the parties and with the server;
each party capable of generating a tokenised message via a bidirectional communication with the server.

[00012] Preferably the tokenised message is generated with reference to a token database located at a remote location.

[00013] Preferably the tokenised message includes at least a first data element, a second data element and a third data element.

[00014] Preferably the first data element comprises identification data for a payor, the second data element comprises identification data for a payee (biller) and the third data element comprises identification currency, denomination and value data.

[00015] Preferably a further tokenised message is generated by either an intermediary entity or the token database.

[00016] Preferably a tokenised message is generated by a bi-directional communication process.

[00017] Preferably the bi-directional communication process is between the token database and an intermediary entity.

[00018] Preferably a step in producing a tokenised message involves de-identifying data.

[00019] Preferably a step in producing a tokenised message involves adding a data element to the message.

[00020] Preferably a step in producing a tokenised message involves removing a data element from the message.

[00021] Preferably a step in producing a tokenised message involves applying an algorithm to the data elements in the message.

[00022] Preferably the token database sequences the tokenised messages.

[00023] Preferably the token database sequences the tokenised messages and transmits the tokenised messages as payment data records to a blockchain settlement system.

[00024] Preferably the blockchain settlement system employs the Ripple protocol.

BRIEF DESCRIPTION OF DRAWINGS

[00025] Embodiments of the present invention will now be described with reference to the accompanying drawings wherein:

[00026] Figure 1A is a block diagram of the entities and intermediaries involved in a prior art electronic settlement system;

[00027] Figure 1B is a data and funds flow according to a prior art settlement system;

[00028] Figure 2A is a data and funds flow diagram according to an indicative embodiment of the present invention;

[00029] Figure 2C is a block diagram of the basic infrastructure and components suited for use with embodiments of the present invention and

[00030] Figure 3 A, B, C comprise block diagrams of the steps in a settlement transaction in accordance with a first preferred embodiment of the present invention

[00031] Figure 4 is a block diagram of salient characteristics of a messaging system 10 of the prior art as compared with the salient messaging characteristics of the system 210 enabled by the code of a second embodiment.

[00032] Figure 5 illustrates the options for data content to be included in tokens in accordance with embodiments of the invention as described above.

[00033] Figure 6 provides a comparison of characteristics of embodiments of the present invention as compared with the prior art Swift-based messaging system.

[00034] Figure 7 is a block diagram in accordance with a further preferred embodiment of the present invention.

[00035] Figure 8 is a block diagram of an implementation of a blockchain arrangement suitable for use with the system of earlier embodiments.

DESCRIPTION OF EMBODIMENTS

[00036] With reference to Figure 1A there is illustrated in block form the basic components of a prior art settlement system. In many transactions there will be an at least first transacting entity 11 which enters into a transaction with an at least second transacting entity 12. The transaction may be as simple as the agreement by the first transacting entity 11 to sell a particular item or service to the second transacting entity 12. Typically the transaction will require settlement for an agreed amount expressed in a Fiat or other currency. In the vast majority of cases the at least first transacting entity 11 will be associated with an at least first intermediary entity 13, in this instance in the form of a bank A and similarly the second transacting entity 12 will be associated with an at least second intermediary entity 14 in this instance in the form of bank B. The first transacting entity 11 will have a first bank account 15 at the first intermediary entity 13 whilst second transacting entity 12 will have a second bank account 16 at second intermediary entity 14. Settlement of any given transaction requires instruction given by first transacting entity 11 to its first intermediary entity 13 to pay an agreed amount from the first bank account 15 to the bank account comprising second bank account 16 of second intermediary entity 14 of second transacting entity 12. For these instructions to be carried out metadata in the form of payment metadata 17 must be assembled at the first intermediary entity 13 sufficient and exhaustive to communicate to the second intermediary entity 14 such that the agreed settlement amount is transmitted from bank A to bank B and more particularly to the specific accounts of the respective first transacting entity 11 and second transacting entity 12.

[00037] A similar transaction may be applied in reverse where the second transacting entity sells a good or service to first transacting entity 11. In such an instance the respective intermediaries, once having received the respective payment metadata 17 and exchanged that metadata 17 may elect to simply pay the difference 18 electronically as between the intermediaries to effect the multiple transactions. In some instances, particularly where the transaction is cross-border-for example the first intermediary entity 13 is in a first country whilst the second intermediary entity 14 is in a second country the metadata 17 may include what is known as a Swift code which is a substantially unique identifier for each intermediary entity involved in the transaction. However, for any given transaction, far more data than merely a unique identifier for each intermediary entity involved in a transaction is required in order for the appropriate settlement amounts to ultimately be recorded in the correct accounts and settle the transaction for the agreed amounts.

[00038] Figure 1B is a data and funds flow diagram of data and funds flow according to a prior art settlement system at the granular level. In this instance, with reference to figure 1B like components are numbered as for figure 1A a given transaction requiring settlement can be embodied as a bill 90 which will include payment data 91 and may include bank facilitation payment data 92 comprising, in this instance, a biller code and a transaction code. Banks which are party to this bank facilitation payment system permit data entry by entity B (or payer B) 12 into a database of bank B 14 by means of a bank application or web interface 14 B. Bank B may then add additional data to form metadata 17 which is sent to a third-party server 93 which utilises metadata 17 to trigger pay (settlement) of bill 90 from payer B bank 14 to biller A bank 13.

Generalised Embodiment:

[00039] With reference to Figure 2C there is illustrated a block diagram of the basic infrastructure and components suited for use with embodiments of the present invention. In this instance like components are numbered as for figure 1 except in the 100 series. So, for example, first transacting entity 11 becomes first transacting entity 111 in this embodiment with reference to figure 2C.

[00040] In this instance a settlement system 110 according to a generalised embodiment includes at least first transacting entity 111 which enters into a transaction with at least a second transacting entity 112. As previously these entities are associated with a respective first

intermediary entity 113 and a second intermediary entity 114 in the form of bank A and bank B. Each of the first transacting entity 111 and a second transacting entity 112 has a respective account 115, 116 at their respective intermediary entities as illustrated in figure 2C

[00041] In this instance, in the event that first transacting entity 111 enters into a transaction with second transacting entity 112 then, at the time of entry into the transaction 120, a token 121 is generated. In this instance the token 121 is generated by at least first digital device 122 communicating with a token database 123. The token database 123 generates a token comprising a data file 124 containing all data that will ultimately be required to settle the transaction 120 including any necessary identifying information for the transacting entity is, their accounts and the intermediary entities. Settlement is effected by communication of the token 121 to bank A and then to bank B together with the appropriate flow of funds.

[00042] With reference to figure 2A at the granular level a bill 190 from a biller 111 directed to a payer 112 contains bill data 191 and also token data of a token 121 residing within a code symbol 194 (in this instance a QR code). The token data includes pointer data pointing to data 195 on token database 123. The data 195 combined with bank ID data 114 permits the creation by token database 123 of a full payment record 196 which can be utilised to cause settlement of the bill 190 as against payer 112 via, in this instance, their respective banks 114, 113.

[00043] With reference to figure 2B the payment data record 196 is utilised has fed into a settlement network such as, for example a network 197 operating under the Ripple protocol thereby permitting substantially real-time settlement across multiple institutions and banks.

First Embodiment:

[00044] With reference to Figures 3 there is illustrated in block diagram form a first preferred embodiment of the present invention by way of a non-limiting example of a transaction. In this embodiment like components are numbered as for the previous embodiments except in the 200 series. So, for example, token 121 becomes token 221.

[00045] With reference to figure 3A the transaction system 210 is activated, as for the previous embodiment, when a transaction 220 is entered into between at least first transacting entity 211 and at least a second transacting entity 212 each dealing, for the purposes of this transaction, through respective intermediary entities 213, 214.

[00046] At the time of and as part of entry into the transaction 220 the first transacting entity 211 accesses token database 223 via digital device 222 executing via a web browser interface or via execution of an application running on a portable digital devices such as a mobile telephone or in a further alternative as a point-of-sale terminal in order to arrange for the database 223 to generate a token 221. In this instance the token 221 will include better data 224 including the recipient named, BIC, IBAN, destination country, mobile number, currency, business type, communication, payment amount. In this instance the token 221 including the metadata 224 is stored in the token database 223. In addition the first transacting entity 211 communicates the token 221 to a digital device 230 associated with second transacting entity 212. In this instance the communication is by way of initial transmission of the token 221 to digital device 222 which then on transmits the token via Internet 231 to digital device 230.

[00047] With reference to figure 3B, when ready to settle the transaction 220 the second transacting entity 212 "logs in" to a portal associated with second intermediary entity 214 and communicates the token 221. In this instance have the login can be executed via a web browser associated with digital device 230 which communicates via Internet 231 the token 221 to a digital processing system 232 (including at least a processor and a memory) associated with second intermediary entity 214. Substantially at the same time as part of seeking to settle the transaction 220:

[00048] Notification: token database 223 notifies second intermediary entity 214 to contact the token database 223 from which it receives a further token 221A.

[00049] Verification: token database 223 communicates with the processing system 232 of second intermediary entity 214 to verify that sufficient funds are located in account 216 as indicated in the meta data 224 to settle the transaction.

[00050] Committing payer funds: payers bank debits payers account: payers bank sends notice to payer bank gateway: payers bank gateway calls token database 223 to get approved token:

[00051] Settlement: gateway of payers bank sends by way of non limiting example XRP (the native currency of the Ripple protocol) to billers bank gateway: payers bank gateway notifies token database 223 of receipt:

[00052] Clearing: payer's bank Nostro account is debited subject to bank institution rules.

[00053] Embodiments of the invention can be implemented utilising the "Ripple" the framework, protocol and gateway-or more generally any blockchain based framework. In a particular form the final settlement process can be enabled through a Ripple frame work thereby to facilitate substantially real-time settlement across multiple institutions and multiple banks.

Second Embodiment:

[00054] Examples of tokenised messages and their generation and transmission are illustrated in pseudocode below. Reference to "sparro" is a reference to an instance of a token database123.

[00055] The previous, meta-data mode is first. It switches to minimal half way through

--

Bank:HSBC >> createUserCode >> Sparro:Sparro

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

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

--

Bank:MayBank >> createUserCode >> Sparro:Sparro

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

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

--

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

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

--

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

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

--

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

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

--

Bank:HSBC >> createInvoiceCode >> Sparro:Sparro

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

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

-

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

```
{ "code": "6tq6wcbad" }
```

--

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

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

```
Abc invoice { amount: { amount: 1000, currency: 'gbp' },  
  payee: '65q3gdd',  
  code: '6tq6wcbad' }
```

--

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

```
{ "amount": { "amount": 1000, "currency": "gbp" }, "payee": "65q3gdd", "code": "6tq6wcbad" }
```

-

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

```
{ "invoice": "6tq6wcbad", "amount": { "currency": "GBP", "amount": 300 } }
```

--

Bank:MayBank >> sendMoney >> BankGateway:MayBank

```
{ "payer": "70wqgx6", "invoice": "6tq6wcbad", "amount": { "currency": "GBP", "amount": 300 } }
```

--

BankGateway:MayBank >> getInvoice >> Sparro:Sparro

```
"6tq6wcbad"
```

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

--

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

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

--

BankGateway:MayBank >> transfer >> BankGateway:HSBC

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

--

BankGateway:HSBC >> incomingTransfer >> Bank:HSBC

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

--

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

{"success":true,"owed":{"GBP":300}}

--

Bank:HSBC >> getInvoice >> Sparro:Sparro

"6tq6wcbad"

--

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

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

--

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

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

--

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

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

XYZ part-paid invoice {

 "payer": "70wqgx6",

 "invoice": "6tq6wcbad",

 "amount": {

 "currency": "GBP",

 "amount": 300

 },

 "id": "ripple-1"

}

--

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

```
{ "invoice": { "amount": { "amount": 1000, "currency": "gbp" }, "payee": "65q3gdd", "code": "6tq6wcb  
ad" }, "transfer": { "payer": "70wqgx6", "invoice": "6tq6wcbad", "amount": { "currency": "GBP", "amo  
unt": 300 }, "id": "ripple-1" } }
```

-

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

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

--

Bank:MayBank >> sendMoney >> BankGateway:MayBank

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

--

BankGateway:MayBank >> getInvoice >> Sparro:Sparro

 "6tq6wcbad"

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

--

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

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

--

BankGateway:MayBank >> transfer >> BankGateway:HSBC

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

--

BankGateway:HSBC >> incomingTransfer >> Bank:HSBC

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

--

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

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

--

Bank:HSBC >> getInvoice >> Sparro:Sparro

```
"6tq6wcbad"
```

--

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

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

--

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

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

--

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

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

XYZ finished paying invoice {

 "payer": "70wqgx6",

 "invoice": "6tq6wcbad",

 "amount": {

 "currency": "GBP",

 "amount": 700

 },

 "id": "ripple-2"

}

--- SWITCHING TO MODE: minimal ---

--

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

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

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

 undefined

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

--

Bank:MayBank >> createUserCode >> Sparro:Sparro

undefined

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

--

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

{"code":"dnt7gec"}

--

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

{"code":"6wwpwuc"}

--

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

{"amount":{"amount":2000,"currency":"gbp"}}}

--

Bank:HSBC >> createInvoiceCode >> Sparro:Sparro

null

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

--

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

{"code":"erwkax1md"}

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

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

```
Abc invoice { amount: { amount: 2000, currency: 'gbp' },
  code: 'erwkax1md',
  payee: 'User:ABC Paper',
  transfers: [] }
```

--

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

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

--

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

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

--

```
Bank:MayBank >> sendMoney >> BankGateway:MayBank
```

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

--

```
BankGateway:MayBank >> getInvoice >> Sparro:Sparro
```

```
"erwkax1md"
```

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

--

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

```
{ "bank": "Bank:HSBC" }
```

--

```
BankGateway:MayBank >> transfer >> BankGateway:HSBC
```

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

--

BankGateway:HSBC >> incomingTransfer >> Bank:HSBC

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

--

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

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

--

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

```
{"invoice":{"amount":{"amount":2000,"currency":"gbp"},"code":"erwkax1md","payee":"User:ABC
```

```
Paper","transfers":[{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":600},"id":"ripple-
```

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

--

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

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

--

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

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

XYZ part-paid invoice {

```
"payer": "6wwpwuc",
```

```
"invoice": "erwkax1md",
```

```
"amount": {
```

```
"currency": "GBP",
"amount": 600
},
"id": "ripple-3"
}
--
User:XYZ Printing >> payInvoice >> Bank:MayBank
  {"invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400}}

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

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

--
BankGateway:MayBank >> getInvoice >> Sparro:Sparro
  "erwkax1md"
(Sending Payment to Invoice - The payment is sent to the bank that created the invoice.)

--
Sparro:Sparro >> getInvoice-reply >> BankGateway:MayBank
  {"bank":"Bank:HSBC"}

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

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

--
BankGateway:HSBC >> incomingTransfer >> Bank:HSBC

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

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

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

--

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

```
{ "invoice":{"amount":{"amount":2000,"currency":"gbp"},"code":"erwkax1md","payee":"User:ABC
```

```
Paper","transfers":[{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP",
```

```
,"amount":600},"id":"ripple-3"},{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":140
```

```
0},"id":"ripple-4"}]], "transfer":{"payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","a
```

--

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

```
{ "payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"i
```

--

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

```
{ "payer":"6wwpwuc","invoice":"erwkax1md","amount":{"currency":"GBP","amount":1400},"i
```

XYZ finished paying invoice {

```
  "payer": "6wwpwuc",
```

```
  "invoice": "erwkax1md",
```

```
  "amount": {
```

```
"currency": "GBP",  
"amount": 1400  
},  
"id": "ripple-4"  
}
```

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

[00056] With reference to figure 4 there is shown a block diagram of salient characteristics of a messaging system 10 of the prior art as compared with the salient messaging characteristics of the system 210 enabled by the code listed above and more broadly described with reference to the earlier embodiments.

[00057] Figure 5 illustrates the options for data content to be included in tokens in accordance with embodiments of the invention as described above.

[00058] Figure 6 provides a comparison of characteristics of embodiments of the present invention as compared with the prior art Swift-based messaging system at a commercial layer 470, a security layer 471 and a technical layer 472.

Further Embodiment

[00059] Figure 7 is a block diagram of a further embodiment. In this instance a distributed ledger 781 operating on blockchain principles provides for transmission of the tokenised message as for previous embodiments.

[00060] In this instance it will be observed that the tokenised transmission distributed ledger 781 operates in parallel with conventional transmission between institution A and institution B.

[00061] Conventional transmission includes transmission of conventional messages utilising the SWIFT protocol. It is also to be noted that institution A and institution B may be subsidiaries of the same institution or may otherwise be closely related. In the alternative they may be completely independent institutions.

[00062] The tokenised message as described in previous embodiments may include information as typically transmitted by the SWIFT or other current acknowledged data transmission systems for transmission of financial information for the purpose of transfer of funds between parties.

[00063] The tokenised message may transmit data which includes some of the data normally included in the conventional message. In alternative forms it may include additional data. In yet alternative forms it may include data not transferred at all in the data normally included in the conventional message.

[00064] The aim, ultimately, is to improve the reliability of the transaction as between the first transacting entity and the second transacting entity and, in some forms, to provide an enhanced capability.

[00065] In the arrangement of figure 7 the data comprising the tokenised message is transmitted via nodes 780 within a blockchain 781.

[00066] In summary, Bank A and Bank B might be branches of the same bank, say HSBC HK and HSBC China (which today use SWIFT for intrabank transfers). So this system could be used within 1 financial institution.

[00067] In one form the purpose of storing the token only in the blockchain is really to both de-identify the information in the blockchain (which is critical for banks), and enable use of existing (SWIFT / ACH / RTGS) or new messaging systems to send the payment instruction in tokenised format. Banks today have significant investment in existing conventional messaging systems and a complete abandonment of these messaging systems would not be feasible. However settlement is still a manual process so linking the conventional messaging system to the 'blockchain' settlement system (via the token) is an important feature of this embodiment. So, in diagram 7 we include a SWIFT/ACH/RTGS connection between the two Financial Institutions (FIs) (or branches) for communication of the token, and the blockchain ledger is common. The data that is required to settle the payment can be provided by the FI's customer or by the FI themselves (say from a core banking system or similar).

[00068] Fig 8 illustrates in block diagram form key components of an implementation of a blockchain structure which may be utilised to implement the system of figure 7.

[00069] Each block includes verified transactions and the blockchain maintains a ledger all prior transactions. The blockchain is duplicated by all the computers on a network.

[00070] The first block in the chain is known as the Genesis block and new blocks can be added in linear and chronological order. From any given block in the chain the information of this genesis block and all blocks that led back to this one can be retrieved. A blockchain is essentially numerous blocks connected through hash chaining where each block is comprised of the following (see figure 8);

- ☐ Timestamp: provides proof that the data in a block existed at a particular time
- ☐ Previous Hash: Essentially a pointer to the previous block
- ☐ Merkle Hash: Summary of all executed transactions
- ☐ Nonce: Individual blocks identity and is an arbitrary number which can only be used once

[00071] The blockchain is managed by a network of distributed nodes where each node contains a copy of the entire blockchain. Each node in the network can add blocks to the chain, where every node is adding blocks at the same point in the chain at the same time. The more nodes that comprise the network the harder it is to disrupt the storage of the blockchain. Unlike centralised systems which rely on a single authority, there is no single point of failure in these distributed nodes network. If you change the content of a block you change its Hash.

[00072] Blockchains can be based on/ operate in association with any one of a number of protocols – for example Ripple or Stellar.

[00073] The above describes only some embodiments of the present invention and modifications, obvious to those skilled in the art, can be made thereto without departing from the scope of the present invention.

CLAIMS

1. A system for settling a transaction electronically; said system comprising:
 - a) at least a first transacting entity;
 - b) at least a second transacting entity;
 - c) at least a first intermediary entity;
 - d) at least a second intermediary entity;
 - e) in the case where the first transacting entity enters into a transaction with the second transacting entity generating a tokenised message at the time of the transaction containing data needed to settle the transaction;
 - f) initiating settlement of the transaction by transmission of the tokenised message between at least two of the entities..
2. The system of claim 1 wherein the tokenised message is generated with reference to a token database located at a remote location.
3. The system of claim 2 wherein the tokenised message includes at least a first data element, a second data element and a third data element.
4. The system of claim 3 wherein the first data element comprises identification data for a payor, the second data element comprises identification data for a payee (biller) and the third data element comprises identification currency, denomination and value data.
5. The system of claim 1 or claim 2 wherein a further tokenised message is generated by either an intermediary entity or the token database.
6. The system of any previous claim wherein a tokenised message is generated by a bi-directional communication process.
7. The system of claim 6 wherein the bi-directional communication process is between the token database and an intermediary entity.
8. The system of any previous claim wherein a step in producing a tokenised message involves de-identifying data.
9. The system of any previous claim wherein a step in producing a tokenised message involves adding a data element to the message.
10. The system of any previous claim wherein a step in producing a tokenised message involves removing a data element from the message.
11. The system of any previous claim wherein a step in producing a tokenised message involves applying an algorithm to the data elements in the message.

12. The system of any previous claim wherein the token database sequences the tokenised messages.
13. The system of any previous claim wherein the token database sequences the tokenised messages and transmits the tokenised messages as payment data records to a blockchain settlement system.
14. The system of claim 13 wherein the blockchain settlement system employs the Ripple protocol.
15. A tokenised message construction system; said system comprising:
 - a) a server in communication with a database and which facilitates communications between a plurality of parties to a transaction;
 - b) each party having a digitised device with which to communicate with other ones of the parties and with the server;
 - c) each party capable of generating a tokenised message via a bidirectional communication with the server.
16. The system of claim 15 wherein the tokenised message is generated with reference to a token database located at a remote location.
17. The system of claim 16 wherein the tokenised message includes at least a first data element, a second data element and a third data element.
18. The system of claim 17 wherein the first data element comprises identification data for a payor, the second data element comprises identification data for a payee (biller) and the third data element comprises identification currency, denomination and value data.
19. The system of claim 15 or claim 16 wherein a further tokenised message is generated by either an intermediary entity or the token database.
20. The system of any one of claims 15 to 19 wherein a tokenised message is generated by a bi-directional communication process.
21. The system of claim 20 wherein the bi-directional communication process is between the token database and an intermediary entity.
22. The system of any one of claims 15 to 21 wherein a step in producing a tokenised message involves de-identifying data.
23. The system of any one of claims 15 to 22 wherein a step in producing a tokenised message involves adding a data element to the message.
24. The system of any one of claims 15 to 23 wherein a step in producing a tokenised message involves removing a data element from the message.

25. The system of any one of claims 15 to 24 wherein a step in producing a tokenised message involves applying an algorithm to the data elements in the message.
26. The system of any one of claims 15 to 25 wherein the token database sequences the tokenised messages.
27. The system of any one of claims 15 to 26 wherein the token database sequences the tokenised messages and transmits the tokenised messages as payment data records to a blockchain settlement system.
28. The system of claim 27 wherein the blockchain settlement system employs the Ripple protocol.
29. The system of any previous claim wherein a second message is transmitted between the intermediaries.
30. The system of claim 29 wherein the second message is tokenised.
31. The system of claim 29 or 30 wherein the second message contains conventional data.
32. The system of claim 29 or 30 or 31 wherein the second message is transmitted by means of a blockchain system.
33. The system of claim 29 or 30 or 31 wherein the second message includes information equivalent to that transmitted by the SWIFT system.
34. The system of claim 29 or 30 or 31 wherein the tokenised message includes additional information beyond that transmitted by the SWIFT system.
35. The system of claim 35 wherein the tokenised message includes information which verifies the security status of at least one party to the transaction.
36. The system of claim 35 wherein the second tokenised message includes information which verifies the security status of both parties to the transaction.

1/13

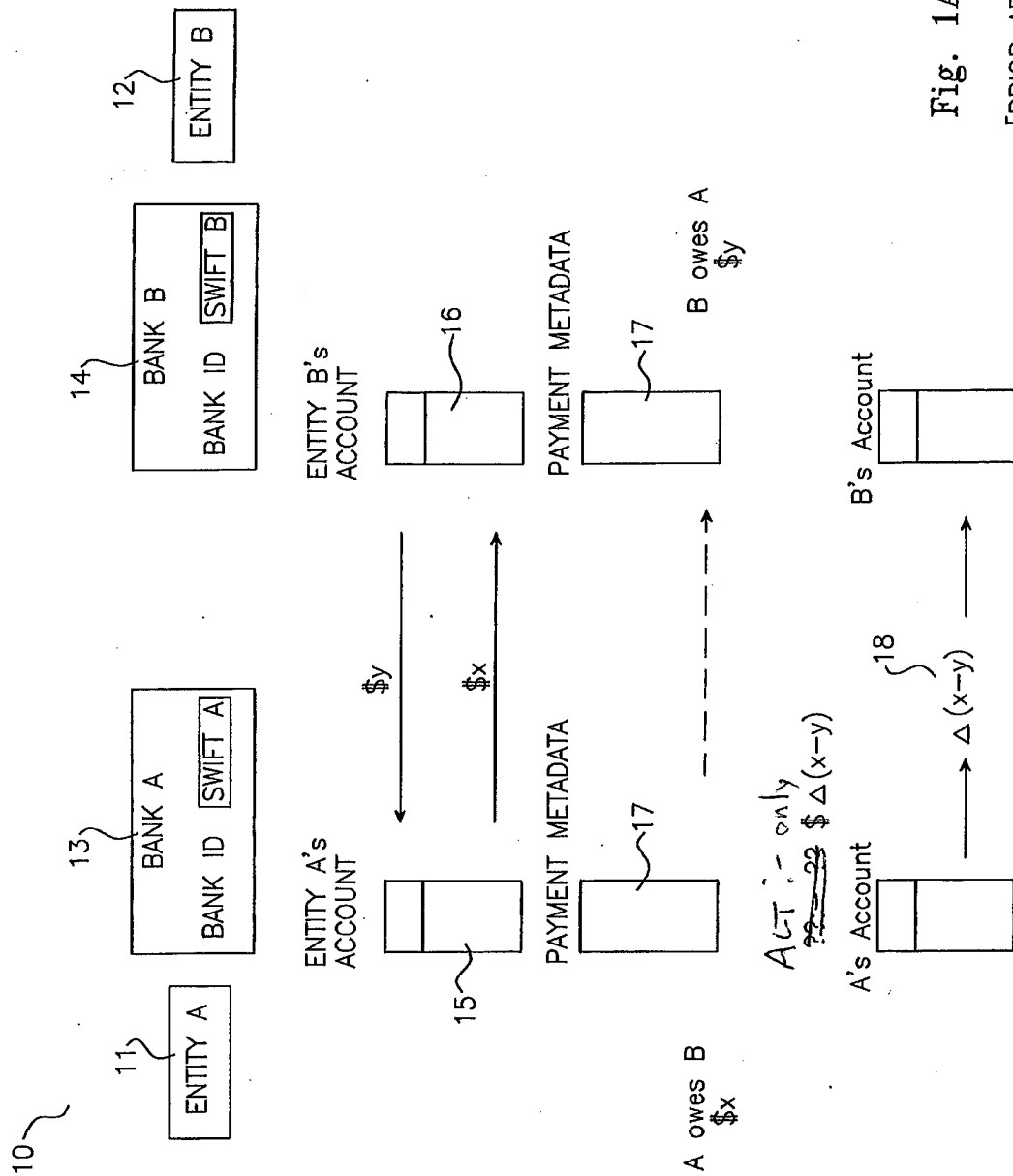


Fig. 1A

[PRIOR ART]

2/13

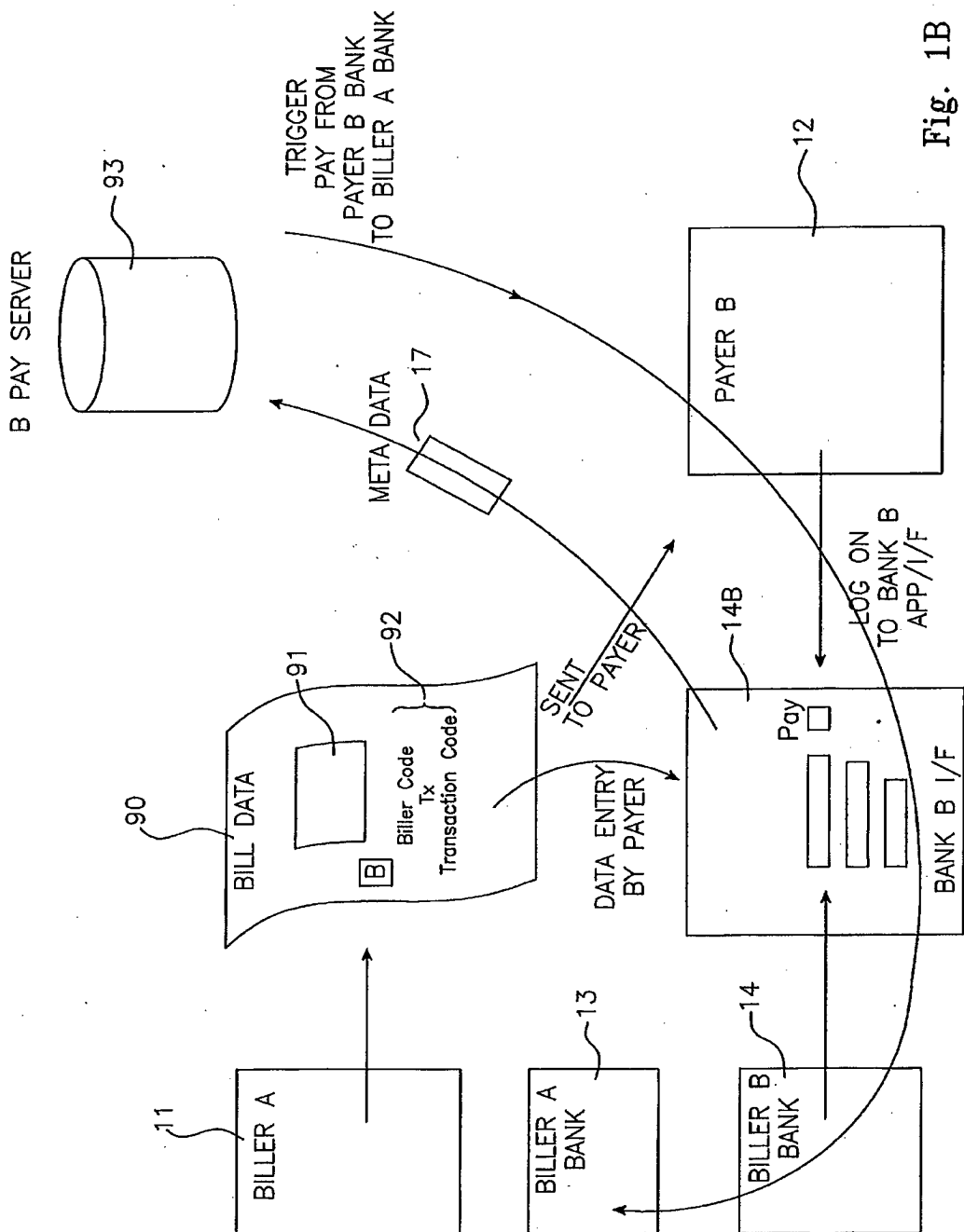


Fig. 1B

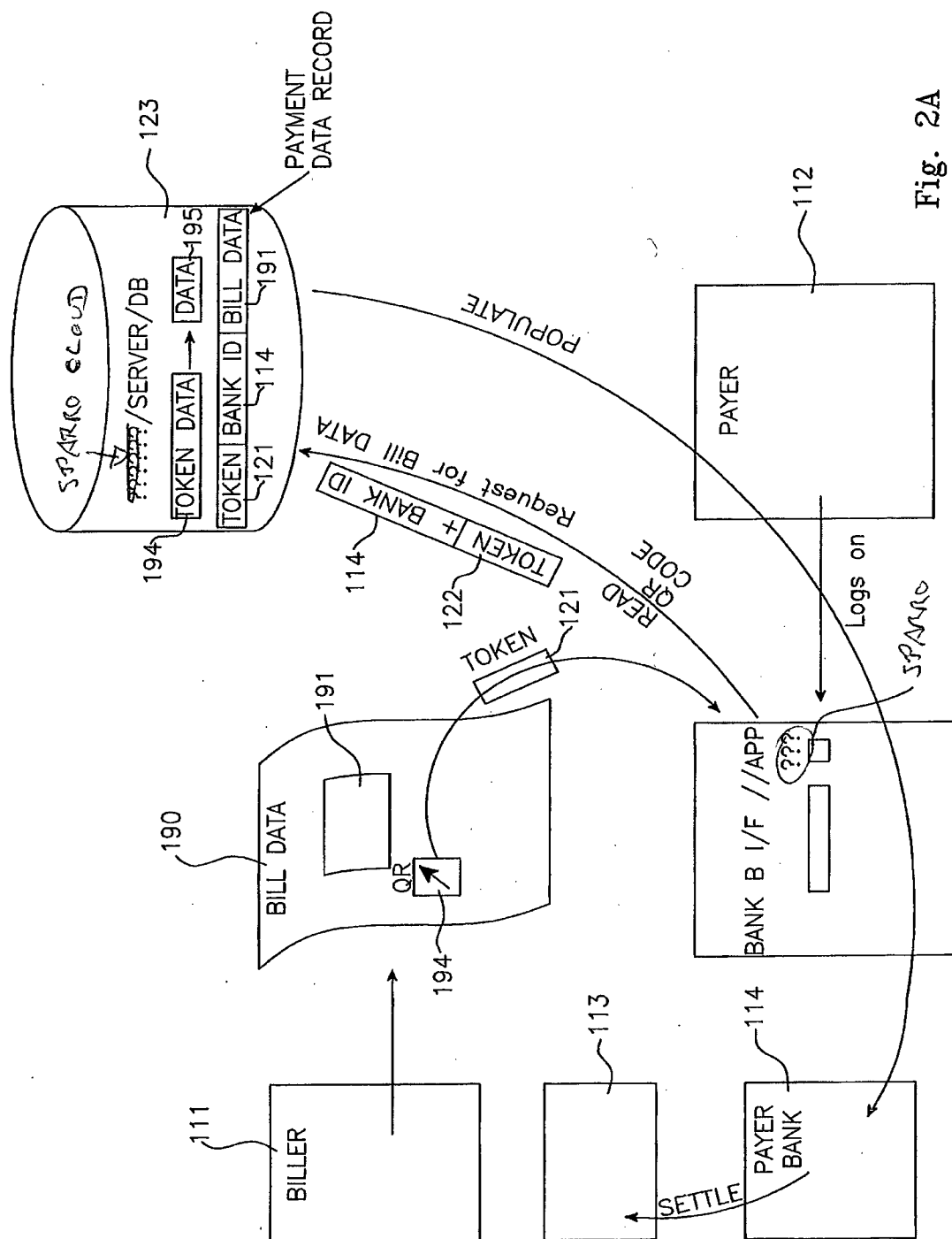


Fig. 2A

4/13

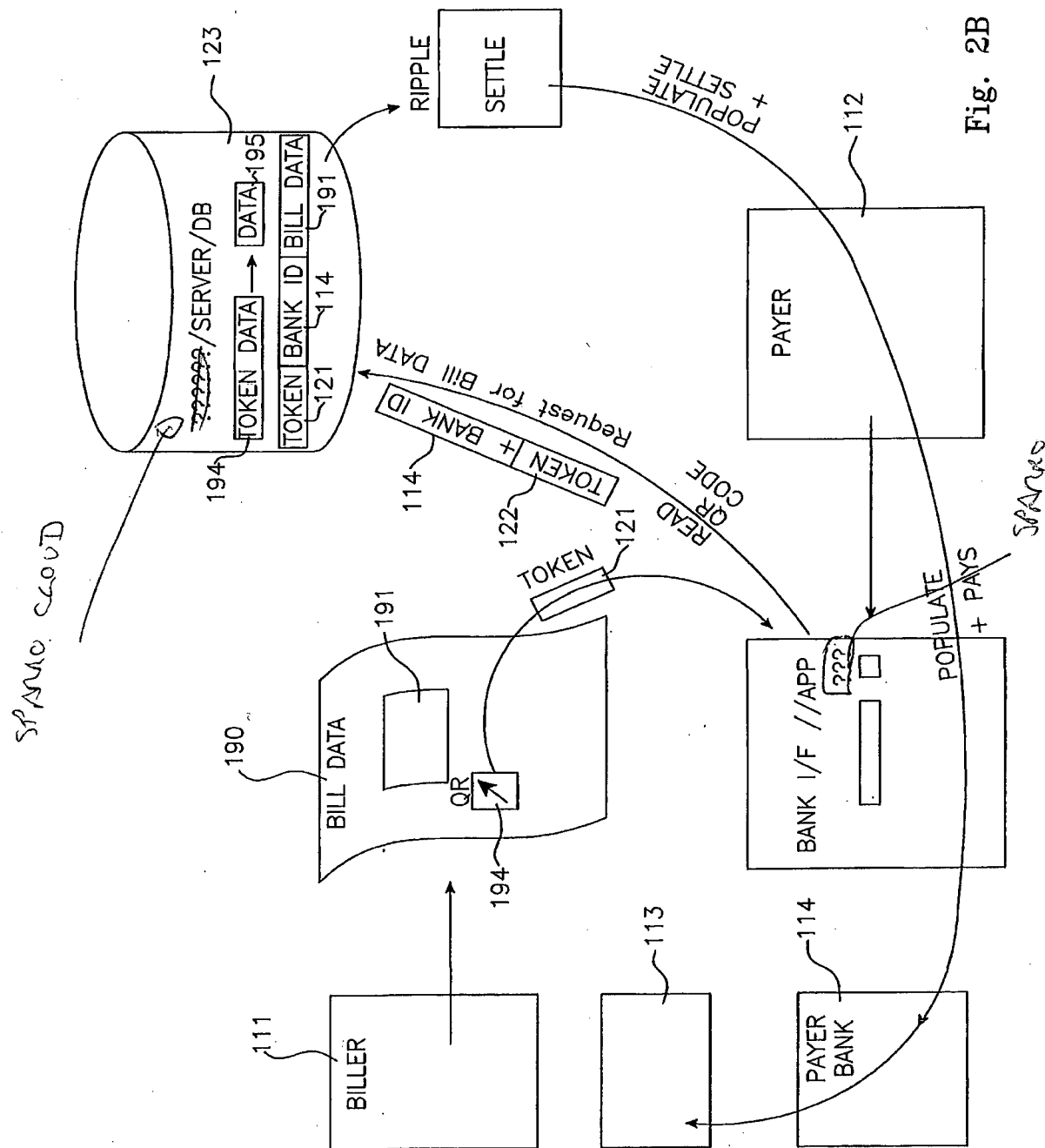


Fig. 2B

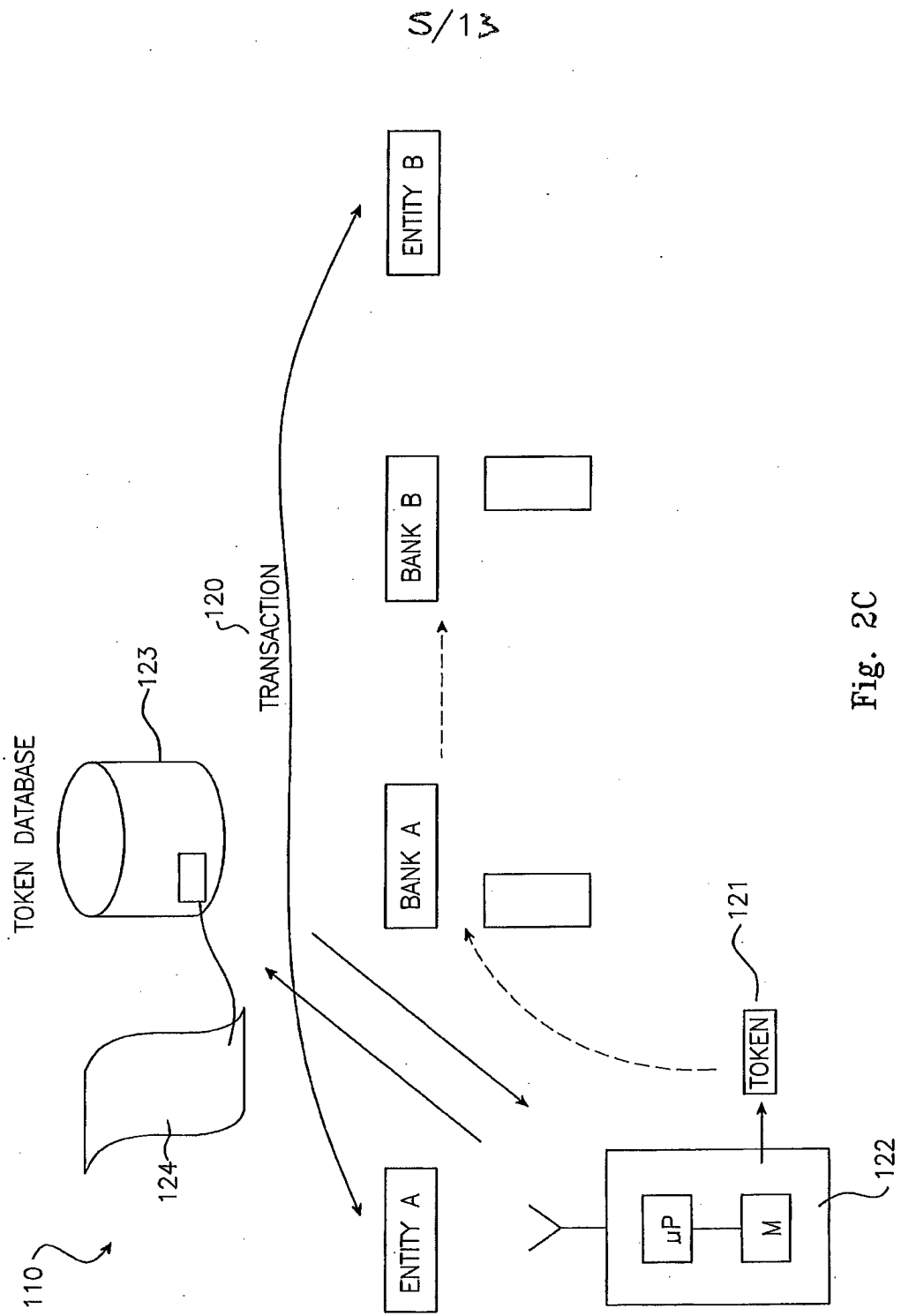


Fig. 2C

6/13

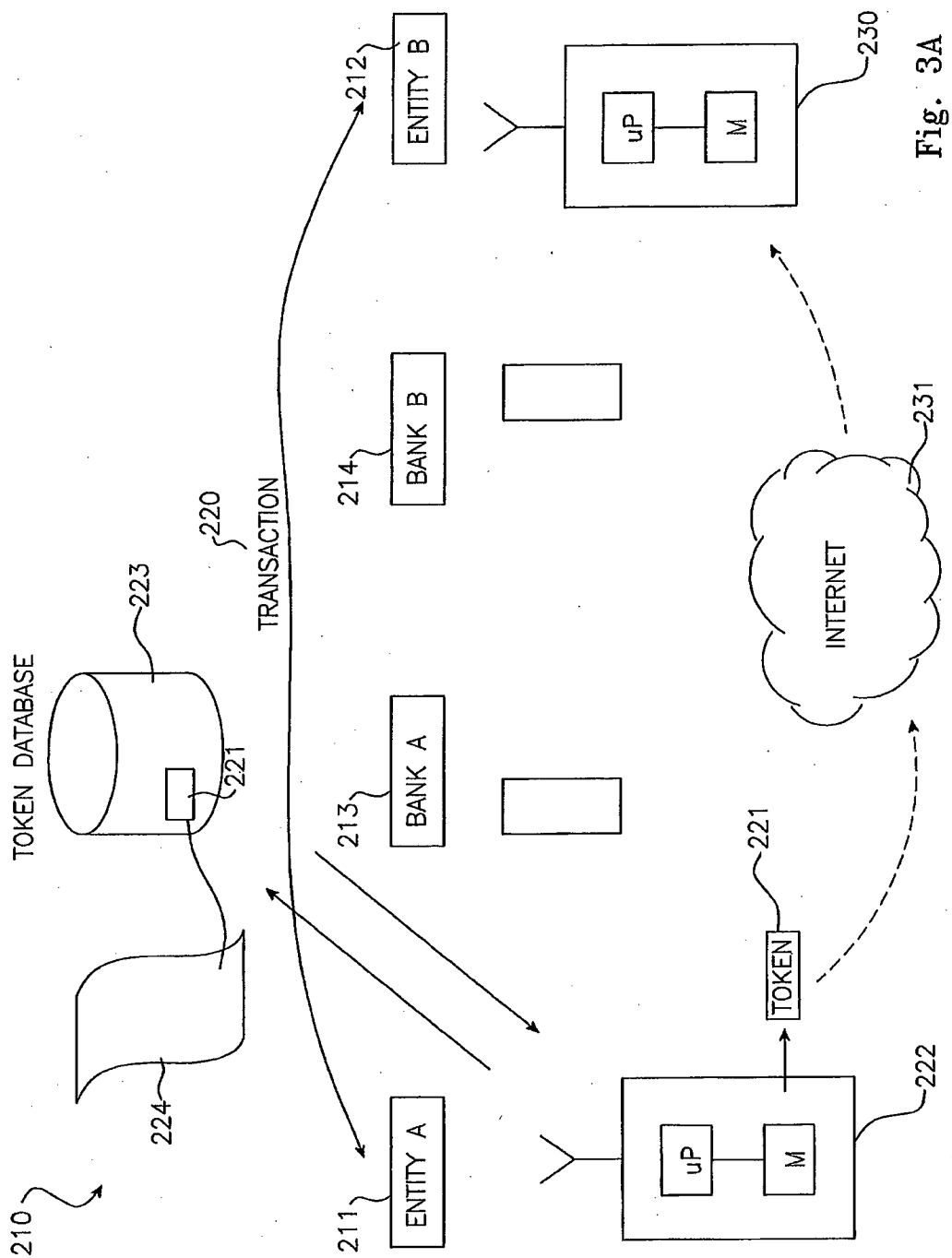
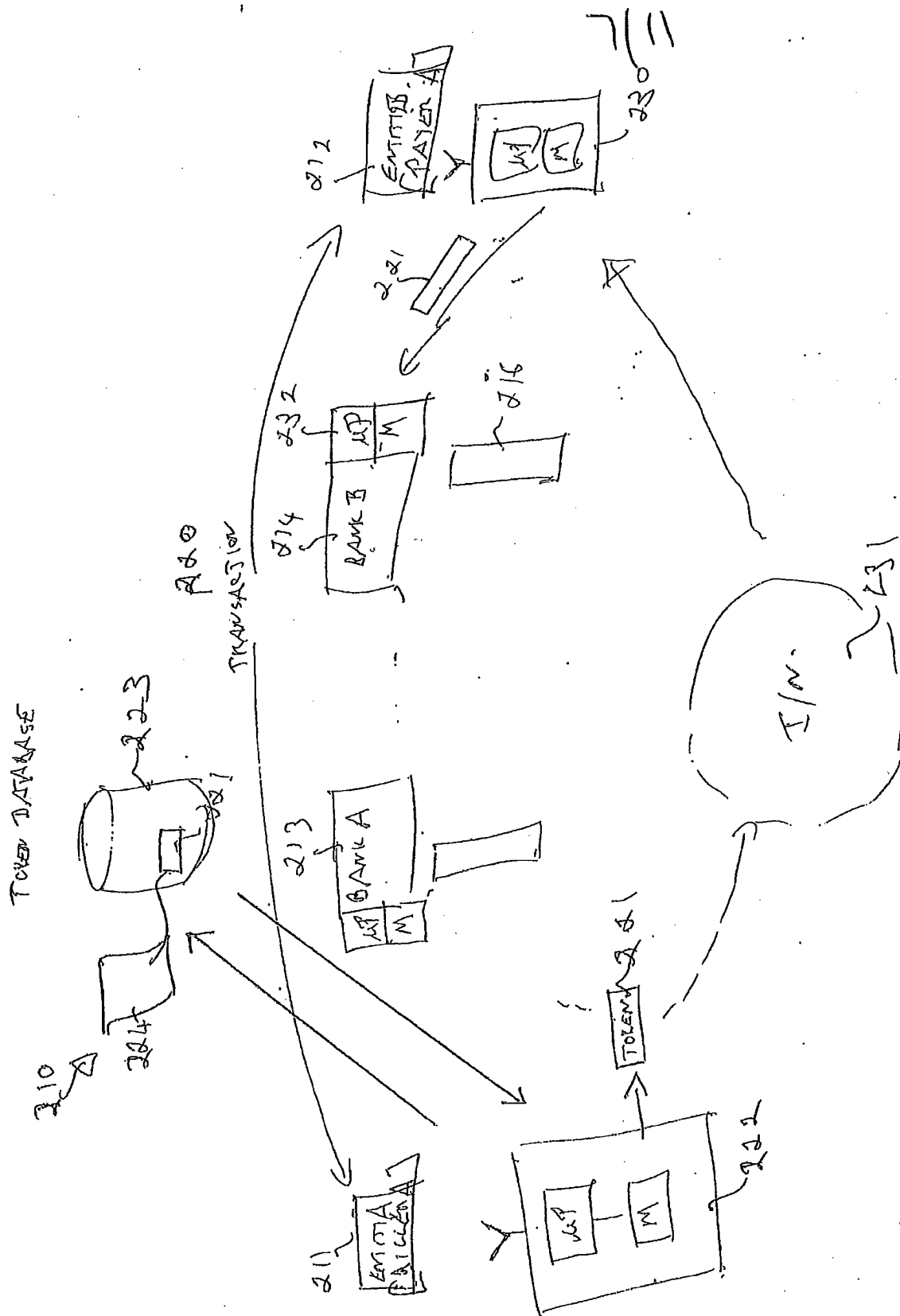


Fig. 3A

7/13




 CT

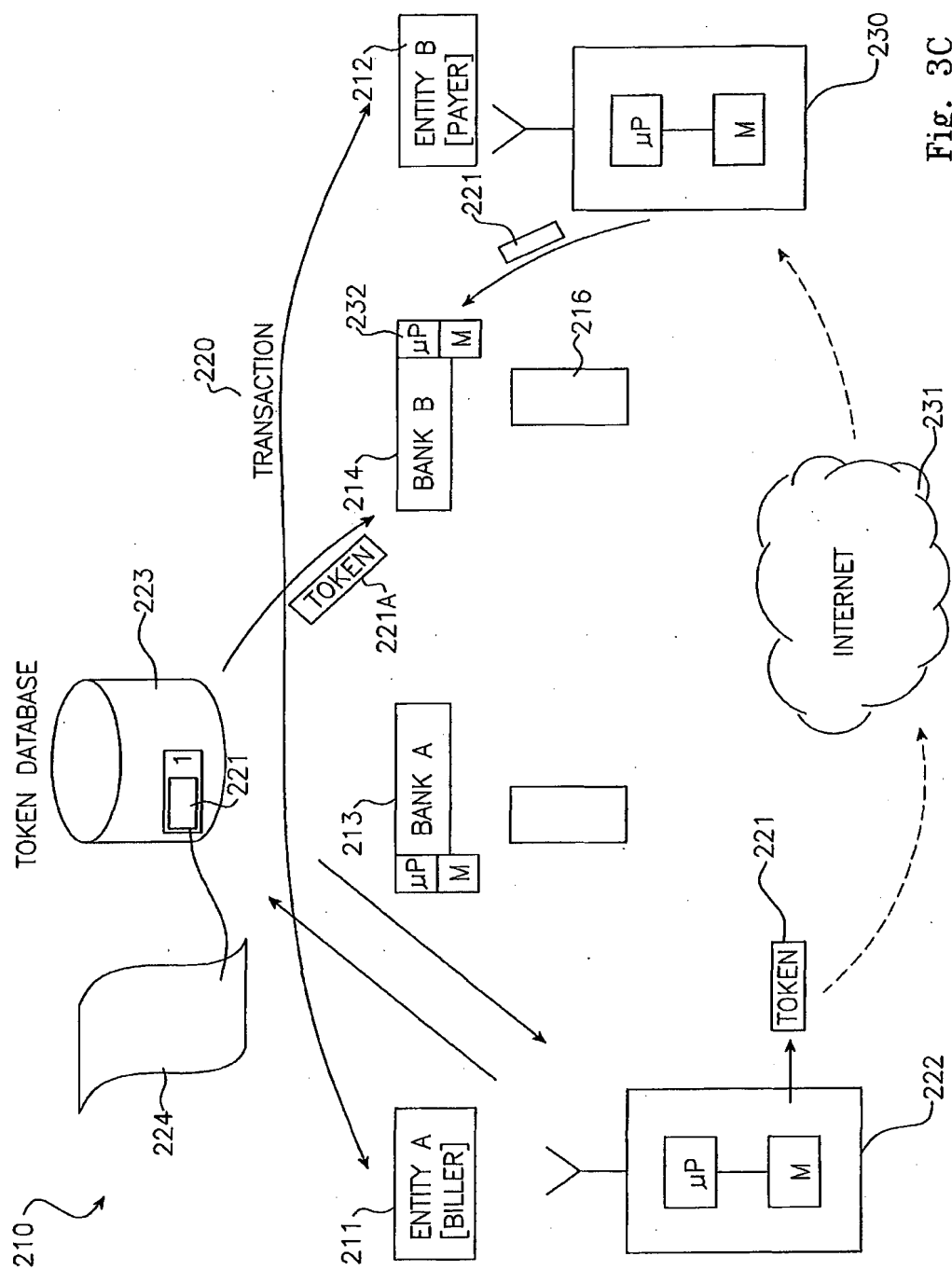


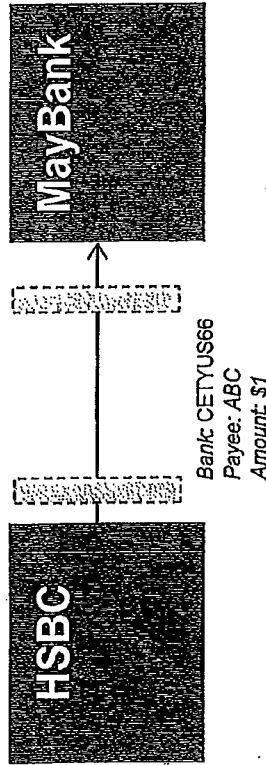
Fig. 3C

Our token system gives power back to Banks run their own shop; with their own, decentralized security management

Existing (SWIFT) system

9/13

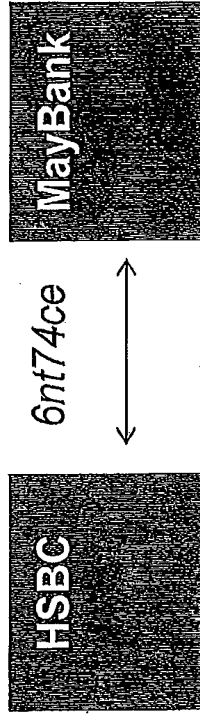
10



(a) Depends on SWIFT infrastructure

Proposed system

210



(a) Bank-originating (cuts costs)

(b) Optional add-on: Data-enriched for PaaS for customers

fig 4

1. Specific to transaction 2. SWIFT codes based on correspondent identifiers, so anyone can do it

We can curate our messaging system to accommodate Bank's risk appetite in relation to user data

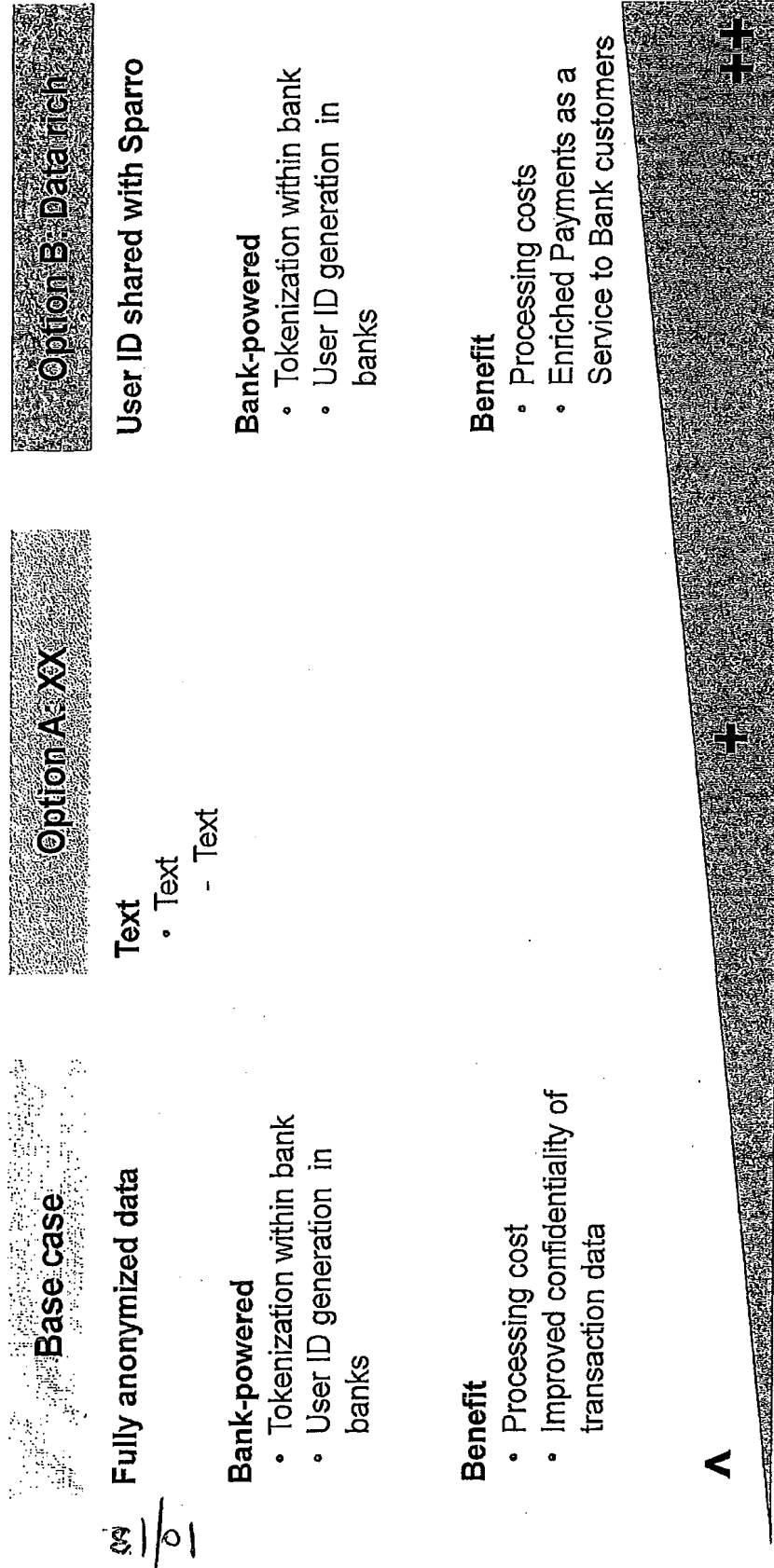


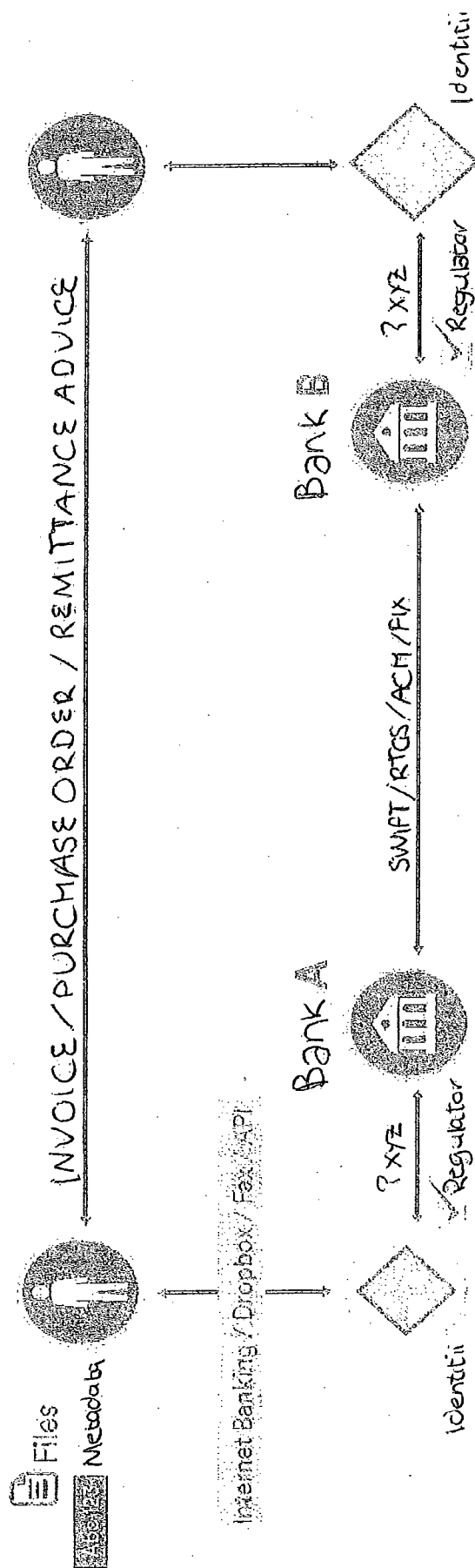
Fig 5

SUMMARY: Benefits to Banks vis-a-vis SWIFT and Ripple

81/11		Issue	SWIFT	Ripple	Proposed
470	{	Commercial	Bypass SWIFT	No competition, given infrastructure focus	1. Banks turn cost centre re SWIFT processing into profit pool 2. <i>Optional add-on:</i> new revenue from e.g. PaaS
		Security	SWIFT-based	Block chain	1. Bank's private system
472	{	Technical	Committed infrastructure spend is slow & expensive	Private gateway establishment	Sparro (anonymized) messaging

fig 6

Diagram 1



12/13

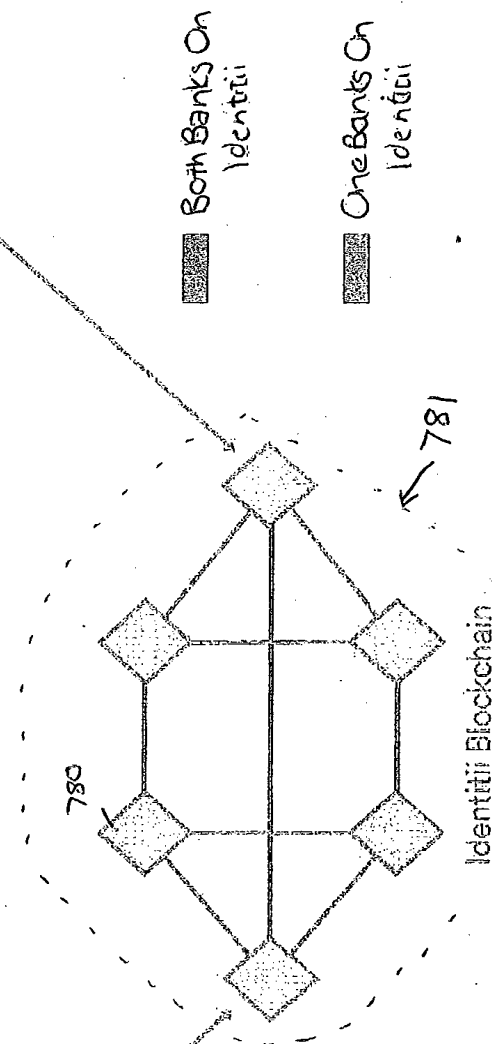
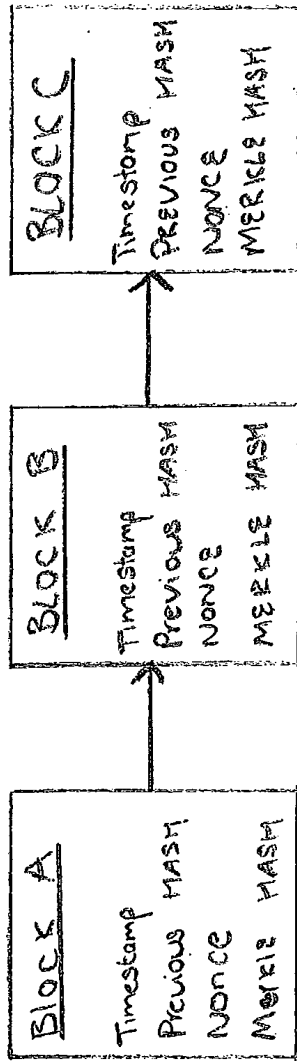
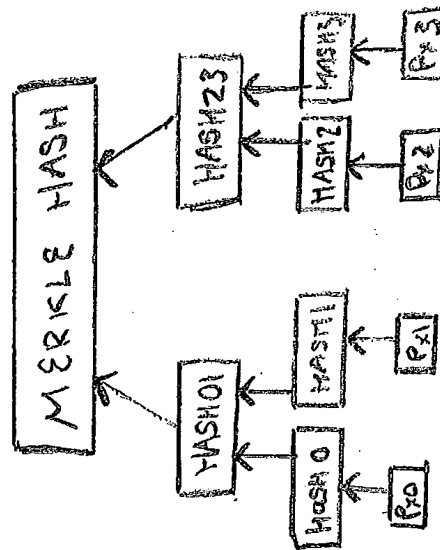


Figure 7

FIGURE 8



where



18/13

DOCUMENT MADE AVAILABLE UNDER THE PATENT COOPERATION TREATY (PCT)

International application number:	PCT/AU2016/000279
International filing date:	12 August 2016 (12.08.2016)
Document type:	Certified copy of priority document
Document details:	Country/Office: AU
	Number: 2016900239
	Filing date: 27 January 2016 (27.01.2016)
Date of receipt at the International Bureau:	27 September 2016 (27.09.2016)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a),(b) or (b-bis)