Distributed and automated exchange between cryptocurrency and traditional currency

Inventor: Brandon Elliott, US

Assignee: Javvy Technologies Ltd., Cayman Islands

REFERENCE TO RELATED APPLICATIONS

[0001] This is a first-filed application.

BACKGROUND OF THE INVENTION

FIELD OF THE INVENTION

[0002] The present invention relates to the field of systems and methods for conducting exchange between cryptocurrency and traditional currency using distributed and cryptographic techniques. Particularly, the present invention relates to the field of systems and methods for conducting exchange between cryptocurrency and traditional currency without the use of an exchange or brokerage. More particularly, the present invention relates to the field of systems and methods for conducting exchange between cryptocurrency and traditional currency in an automated manner on a distributed network, without the use of an exchange or brokerage.

MOTIVATION AND DESCRIPTION OF RELATED ART

[0003] A cryptocurrency (or cryptographic currency) is a digital currency in which encryption techniques are used to verify transaction and regulate the generation of currency. Numerous cryptographic currencies have become available since the creation of the first cryptocurrency, Bitcoin, in 2009, such as Ether, Litecoin, Dash, and so on. The transactions of these cryptocurrencies are typically stored on a ledger or software block-chain and validated by a peer-to-peer distributed network of computers. Using such a distributed network removes the need for a

third party to validate transactions. The increasing popularity of cryptocurrencies reflects the desire for an alternative to traditional currencies, e. g. FIAT money, so that fast, low-cost, universally available transaction of currency is available to online users, operating independently of a central bank.

[0004] A virtual cryptographic wallet, (hereinafter termed "crypto wallet" or "wallet"), is a tool for cryptocurrency users to store cryptographic keys and cryptographic currency, and to facilitate online transactions including sending and receiving of a cryptocurrency. Currently, however, cryptocurrencies cannot be conveniently purchased or sold. Exchange between cryptocurrencies and FIAT money is usually conducted by using the service of an asset exchange or online brokerage company. A user needs to first register and verify an account with the exchange or brokerage company and then add a number of payment options such as credit or debit cards, bank accounts, or wire transfers of funds. Typically the account verification process requires a copy of the user's driver's license and detailed personal information. After the account is verified, further details from the user may be required to expand the buying limits. This process is both time consuming (usually taking days or weeks) and costly for the users, and may potentially result in personal information breaches and identity theft. In addition, the centralized exchange process in part defeats the purpose of the decentralized, secure nature of cryptocurrencies since the exchange transactions are conducted via traditional means, and are associated with the usual risks of fraudulent transactions before the settlement. The lack of easy-to-use and secure currency exchange options have become an important limiting factor holding cryptocurrency back from reaching the mainstream.

[0005] Therefore, it is desirable to develop a crypto wallet integrated with currency exchange functions that are secure and automated, operating on a distributed network, and independent of a third-party exchange or brokerage service.

SUMMARY OF THE INVENTION

[0006] The objective of the present invention to provide a crypto wallet integrated with currency exchange functions that are secure and automated, operating on a distributed network, and independent of a third-party exchange service.

[0007] In one aspect of the present invention, in addition to the functions of a typical crypto wallet, a distributed and automated exchange between cryptocurrency and FIAT money is integrated within the wallet. The process does not rely on a third-party exchange or brokerage service, largely eliminating the cost, time-delay, and risk associated with traditional settlement technologies.

[0008] In another aspect of the present invention, the cross-currency exchange function is accomplished by a 2-phase process. In the first phase, the wallet generates an order, signs it cryptographically, and broadcasts it to the network. In the second phase, the network nodes confirm each order transaction request and completes the transaction.

[0009] In yet another aspect of the present invention, at each phase of the transaction process, additional security and verification measures may be taken to ensure the legitimacy of the transaction.

[0010] The above invention aspects will be made clear in the drawings and detailed description of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] Fig. 1 is an overall system layout of an embodiment of the present invention.

[0012] Fig. 2 is a flowchart showing the overall cross-currency exchange process of an embodiment of the present invention.

[0013] Fig. 3 is a flowchart showing further details of the crypto transfer settlement process of an embodiment of the present invention.

[0014] Fig. 4 is a flowchart showing further details of the FIAT transfer settlement process of an embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0015] The disclosed technology provides a crypto wallet integrated with distributed and automated exchange operation between cryptocurrency and FIAT money. The exchange may be performed between crypto wallets, or importantly, between a crypto wallet and a non-crypto wallet entity, such as a bank account via banking APIs and verified through a distributed network.

[0016] The processes described in this disclosure can be implemented by software, by programmable circuitry configured by software and/or firmware, or entirely by special-purpose circuitry, or in a combination of such forms.

[0017] In the detailed description, numerous specific details are set forth in order to provide a thorough understanding of the invention. However, it will be understood by those skilled in the art that these are specific embodiments, and that the present invention may be practiced also in different ways that embody the characterizing features of the invention as described herein. Additionally, some well-known structures or functions may not be shown or described in detail, so as to avoid unnecessarily obscuring the relevant description of the various embodiments.

[0018] Fig. 1 is an overall system layout of an embodiment of the present invention. A crypto wallet 100 is in communication with a distributed network 200 with multiple peer nodes 220. The distributed network 200 communicates with a banking API 720 of a financial institution 700 and serves as the communication pathway between the crypto wallet 100 and the bank API 720. The crypto wallet 100 may hold one or more types of cryptocurrencies 110. The banking API is in communication with one or more accounts 750, which may hold FIAT cash or other asset positions.

[0019] Fig. 2 shows a flowchart of the overall cross-currency exchange process of an embodiment of the present invention. First the wallet 100 cryptographically signs a BUY or SELL order and broadcasts the order to the distributed network 200 (301), then the peer nodes 220 of the network 200 confirm the validity of the broadcasted transaction (305). In the next step, a decision is made by the peer nodes 220 whether the broadcasted message is a BUY order (309). In this illustrated embodiment, a BUY order is a conversion from FIAT money to cryptocurrency, and alternatively, a SELL order is a conversion from cryptocurrency to FIAT money.

[0020] If the peer nodes 220 confirm that it is a BUY order in step 309, then a verification step is optionally performed to check if the crypto address is a known "bad" address (320), i. e., if the crypto address is associated with an entity on a blacklist provided by one or more monitory or regulatory agencies, for example, by the Office of Foreign Assets Control (OFAC). If the crypto address is indeed on a blacklist, the transaction is cleared from the memory pool (mempool) and the wallet 100 with a returned failure message and reasoning (450) and the transaction request is terminated (600). If the crypto address initial check is passed, the FIAT transfer settlement checking process is started. In this process, the peer nodes periodically check for confirmation of funds settlement for a given transaction ID (410) to determine whether the funds have been cleared (435). Once the funds are cleared, the crypto transfer is initiated and the wallet order is updated (445). In this case, the crypto purchase is successfully made and the process is terminated (600). During the period of time when the funds are not cleared, a timeout check (440) is made to see if a predetermined time limit has been reached. Within the time limit, the check for settlement confirmation step (410) is repeated. When the time limited has been reached without a confirmation of cleared funds, the BUY order expires and the transaction is cleared from the memory pool (mempool) and the wallet 100 with a returned failure message and reasoning (450) and the transaction request is terminated (600).

[0021] If the peer nodes 220 confirm that it is a SELL order in step 309, a verification step is optionally performed to check if the bank account or the account holder name is on a blacklist provided by one or more monitory or regulatory agencies, for example, by the Office of Foreign Assets Control (OFAC). If the bank account or account holder name is indeed on a blacklist, the

SELL order is cleared from the memory pool (mempool) and the wallet 100 with a returned failure message and reasoning (550) and the transaction request is terminated (600). If initial account check is passed, the crypto transfer settlement checking process is started. In this process, the peer nodes 220 periodically check for confirmation of crypto transfer to incoming crypto address for the given transaction ID (510) to determine whether the funds have been cleared (535). Once the funds are cleared, the FIAT transfer is initiated and the wallet order is updated (545). The crypto SELL is successfully made and the process is terminated (600). During the period of time when the funds are not cleared, a timeout check (540) is made if a predetermined time limit has reached. Within the time limit, the check for settlement confirmation step (510) is repeated. When the time limited has been reached without a confirmation of cleared funds, the SELL order expires and the transaction is cleared from the memory pool (mempool) and the wallet 100 with a returned failure message and reasoning (550) and the transaction request is terminated (600).

[0022] Fig. 3 is a flowchart showing further details of the crypto transfer settlement process 400 of an embodiment of the present invention. First, the peer nodes 220 are checked to see whether X number of blockchain peer nodes confirm the transaction (401). Here, X is a predetermined number chosen for a specific embodiment of the system. The choice of X may be varied depending on one or multiple factors of the system specification. When the confirmation is not reached by all X number of nodes, the peer nodes 220 repeat the checking for blockchain confirmation (470 and 475) until a timeout is reached (477). In the timeout scenario, the process is aborted with termination (490). When all X peer nodes 220 confirm the transaction order, the FIAT transfer is confirmed via the corresponding banking API 720, and the wallet 100 is updated with the pending transfer (460). Next if a confirmation is returned by the banking API 720 (465), the transfer confirmation is successful and the process is terminated (490). If the banking API 720 does not confirm the transaction, an error message is relayed to the wallet order and the administrator is notified (467), the process is aborted with termination (490).

[0023] Fig. 4 is a flowchart showing further details of the FIAT transfer settlement process 500 of an embodiment of the present invention. The system keeps waiting for a confirmation communication from the financial institution 700, for example, via an email message (501). The

peer nodes 220 of the distributed network 200 keep checking for email from the financial institution 700 (560). When the peer nodes determine that the email exist (562), they check whether the transaction ID matches the intended transaction (566), and if so, check if the funds have been settled (568). When the fund settlement is confirmed by the peer nodes 220, the checking process returns (590) with a positive result. Both the email checking 562 and fund settlement checking 568 processes are repeated until a positive return or a when a predetermined time limited is reached, i. e. a timeout. When the timeout is reached for either processes 562 or 566, the settlement checking process is aborted with termination (590).

[0024] The foregoing description and accompanying drawings illustrate the principles, preferred or example embodiments, and modes of assembly and operation, of the invention; however, the invention is not, and shall not be construed as being exclusive or limited to the specific or particular embodiments set forth hereinabove.

ABSTRACT

The present invention provides a crypto wallet integrated with secure and automated currency exchange in a process that is independent of a third-party exchange service. Particularly, a distributed and automated exchange between cryptocurrency and FIAT money is integrated within the wallet. The cross-currency exchange function is accomplished by a 2-phase process. In the first phase, the wallet generates an order, signs it cryptographically, and broadcasts it to the network. In the second phase, the network nodes confirm each order transaction request and completes the transaction. At each phase of the transaction process, security and verification measures are taken to ensure the legitimacy of the transaction.

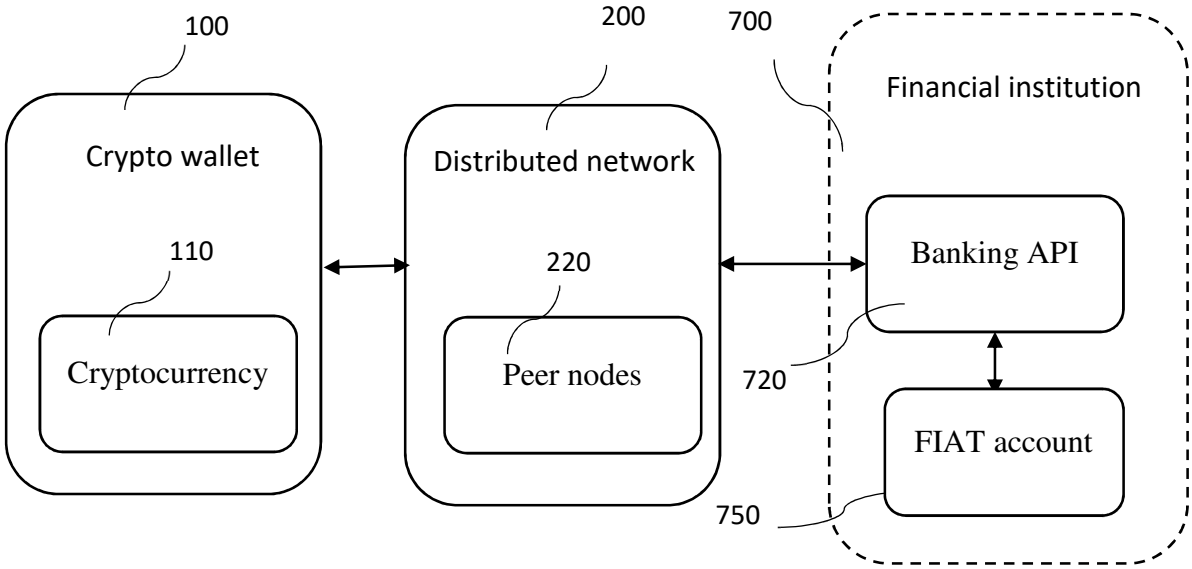
100
Crypto wallet
110
Cryptocurrency
200
Distributed network
220
Peer nodes
700
Financial institution
Banking API
720
FIAT account
750

Fig. 1

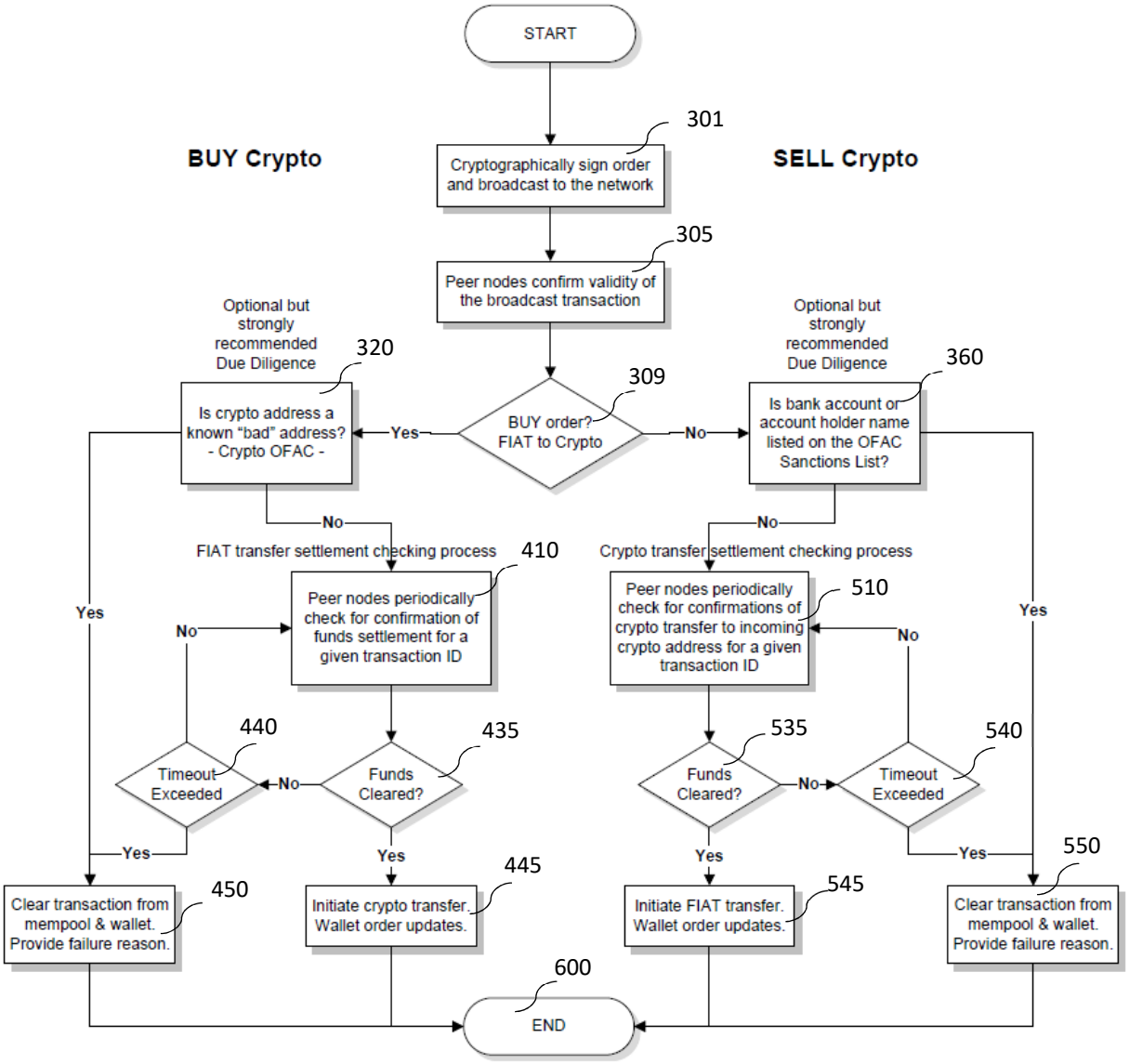
START
301
BUY Crypto
Cryptographically sign order and broadcast to the network
SELL Crypto
305
Peer nodes confirm validity of the broadcast transaction
Optional but strongly recommended Due Diligence
320
Is crypto address a known "bad" address? - Crypto OFAC -
309
BUY order? FIAT to Crypto
Yes
No
Optional but strongly recommended Due Diligence
360
Is bank account or account holder name listed on the OFAC Sanctions List?
No
No
FIAT transfer settlement checking process
410
Peer nodes periodically check for confirmation of funds settlement for a given transaction ID
Crypto transfer settlement checking process
510
Peer nodes periodically check for confirmations of crypto transfer to incoming crypto address for a given transaction ID
Yes
No
No
Yes
440
Timeout Exceeded
No
435
Funds Cleared?
535
Funds Cleared?
No
540
Timeout Exceeded
Yes
Yes
Yes
Yes
450
Clear transaction from mempool & wallet. Provide failure reason.
445
Initiate crypto transfer. Wallet order updates.
545
Initiate FIAT transfer. Wallet order updates.
550
Clear transaction from mempool & wallet. Provide failure reason.
600
END

Fig. 2

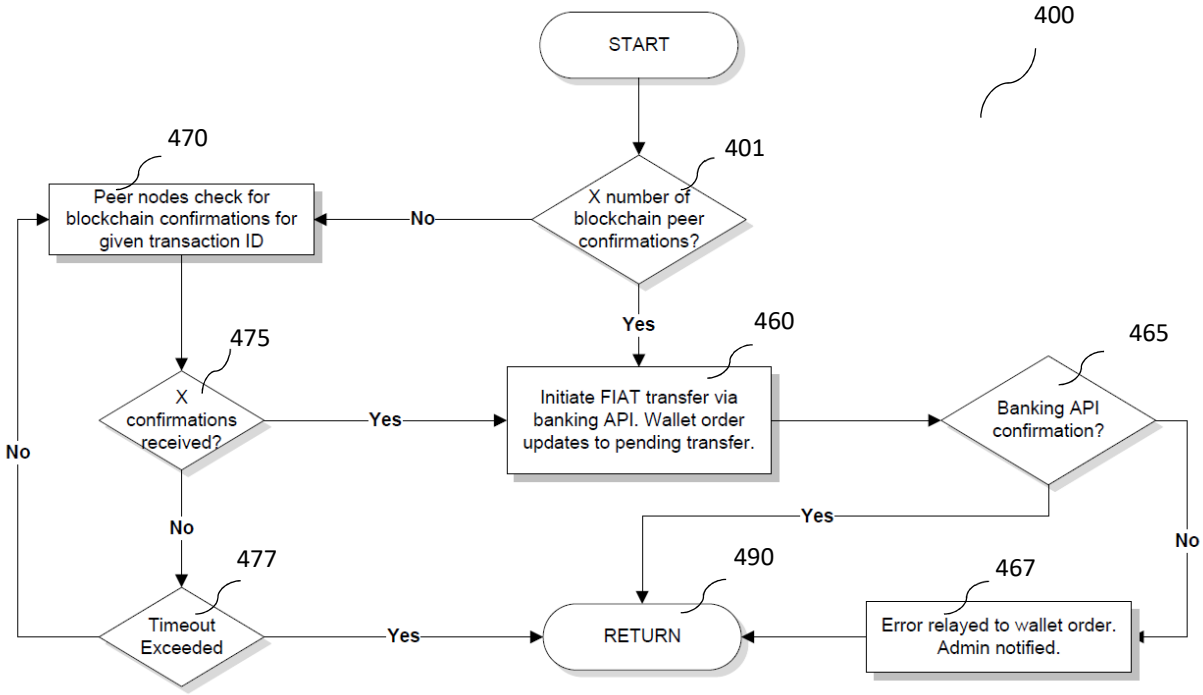
400
START
401
X number of blockchain peer confirmations?
No
470
Peer nodes check for blockchain confirmations for given transaction ID
Yes
460
Initiate FIAT transfer via banking API. Wallet order updates to pending transfer.
465
Banking API confirmation?
Yes
No
467
Error relayed to wallet order. Admin notified.
490
RETURN
Yes
475
X confirmations received?
No
Yes
No
477
Timeout Exceeded
Yes
No

Fig. 3

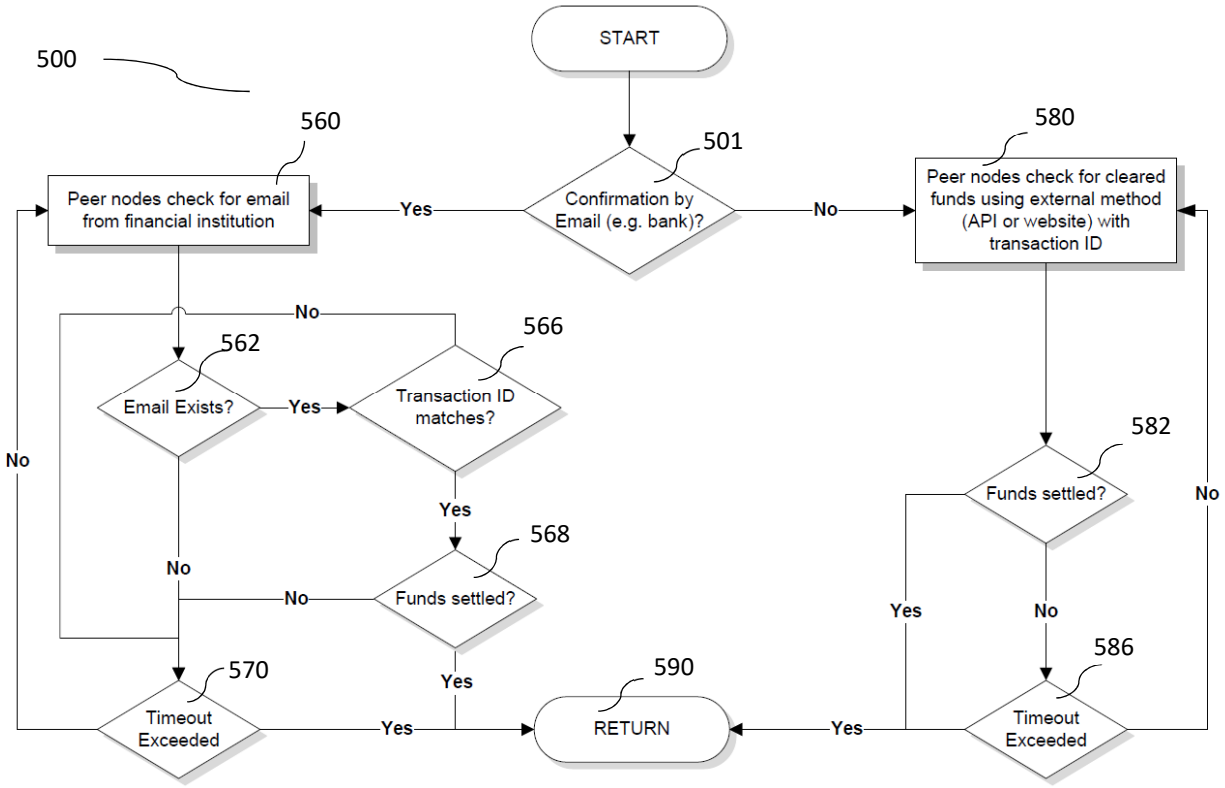
500
START
560
Peer nodes check for email from financial institution
Yes
501
Confirmation by Email (e.g. bank)?
No
580
Peer nodes check for cleared funds using external method (API or website) with transaction ID
No
562
Email Exists?
Yes
566
Transaction ID matches?
Yes
582
Funds settled?
No
No
No
568
Funds settled?
No
Yes
No
Yes
586
Timeout Exceeded
570
Timeout Exceeded
Yes
590
RETURN
Yes

Fig. 4