

PUSH INTERACTION USING CRYPTOCURRENCY EXCHANGE

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] None.

BACKGROUND

5 **[0002]** In certain circumstances, it is desirable to transfer value in one form of currency from one person to another person in another form of currency. For example, it can be desirable to send a cryptocurrency amount to a second user using fiat currency held by a first user. Such transfers, however, can take a significant amount of time. For example, if the first user uses an account such as a demand account as a funds source,
10 a transfer such as an ACH transfer can take one, two, or three days to complete. As such, it would be desirable to reduce the transaction time for a transaction that transfers one form of currency using another form of currency. In addition, the infrastructure to perform such transfers on a timely basis is not readily available.

[0003] Embodiments of the invention are directed to addressing these and other
15 problems, individually and collectively.

BRIEF SUMMARY

[0004] One embodiment can include a method comprising: receiving, by a second authorizing entity computer from a first authorizing entity computer, a push transfer message comprising a credential and an amount; adjusting, by the second
20 authorizing entity computer, a value of an account based on the amount in the push transfer message; and transmitting, by the second authorizing entity computer to a cryptocurrency exchange computer, a credit message comprising the credential and the amount, wherein the cryptocurrency exchange computer communicates with an alias directory computer to obtain an alias associated with credential, and then credits a
25 cryptocurrency account associated with the alias in an amount of cryptocurrency corresponding to the amount in the push transfer message.

[0005] Another embodiment of the invention includes a second authorizing entity computer comprising: a processor; and a non-transitory computer readable medium, the

non-transitory computer readable medium comprising code, executable by the processor, for performing a method comprising: receiving, from a first authorizing entity computer, a push transfer message comprising a credential and an amount; adjusting a value of an account based on the amount in the push transfer message; and transmitting, to a cryptocurrency exchange computer, a credit message comprising the credential and the amount, wherein the cryptocurrency exchange computer communicates with an alias directory computer to obtain an alias associated with credential, and then credits a cryptocurrency account associated with the alias in an amount of cryptocurrency corresponding to the amount in the push transfer message

[0006] Another embodiment includes a method comprising: receiving, by an exchange computer from a second authorizing entity computer, a credit message comprising a credential and an amount, the amount being present in a push transfer message transmitted by a first authorizing entity computer and comprising a credential and the amount; communicating, by the exchange computer with an alias directory computer to obtain an alias associated with credential; receiving, by the exchange computer, the alias; and adjusting, by the exchange computer, a cryptocurrency account associated with the alias in an amount of cryptocurrency corresponding to the amount in the push transfer message.

[0007] Another embodiment includes an exchange computer comprising: a processor; and a computer readable medium coupled to the processor, the computer readable medium comprising code executable by the processor for performing a method comprising: receiving, from a second authorizing entity computer, a credit message comprising a credential and an amount, the amount being present in a push transfer message transmitted by a first authorizing entity computer and comprising a credential and the amount; communicating with an alias directory computer to obtain an alias associated with credential; receiving the alias; and adjusting a cryptocurrency account associated with the alias in an amount of cryptocurrency corresponding to the amount in the push transfer message.

[0008] Further details regarding embodiments of the invention can be found in the Detailed Description and the Figures.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] FIG. 1 shows a block diagram of a system and overlaid method for registering to obtain a credential according to an embodiment of the invention.

5

[0010] FIG. 2 shows a block diagram of a system and overlaid method for performing a transaction according to an embodiment of the invention.

[0011] FIG. 3 shows a block diagram of a user device according to an embodiment.

5 **[0012]** FIG. 4 shows a block diagram of an exchange computer according to an embodiment.

[0013] FIG. 5 shows a block diagram of an authorizing entity computer according to an embodiment.

[0014] FIG. 6 shows a portion of a blockchain according to an embodiment.

10

DETAILED DESCRIPTION

[0015] Prior to discussing specific embodiments of the invention, some terms may be described in detail.

[0016] A “user” may include an individual. In some embodiments, a user may be associated with one or more personal accounts and/or mobile devices. The user may
15 also be referred to as a cardholder, account holder, or consumer.

[0017] A “user device” may comprise any suitable electronic device that may be transported and operated by a user, which may also provide remote communication capabilities to a network. Examples of remote communication capabilities include using a mobile phone (wireless) network, wireless data network (e.g., 3G, 4G or similar
20 networks), Wi-Fi, Wi-Max, or any other communication medium that may provide access to a network such as the Internet or a private network. Examples of user devices include mobile phones (e.g., cellular phones), PDAs, tablet computers, net books, laptop computers, personal music players, hand-held specialized readers, etc. Further examples of user devices include wearable devices, such as smart watches, fitness
25 bands, ankle bracelets, rings, earrings, etc., as well as automobiles with remote communication capabilities. A user device may comprise any suitable hardware and software for performing such functions, and may also include multiple devices or components (e.g., when a device has remote access to a network by tethering to another device - i.e., using the other device as a modem – both devices taken together
30 may be considered a single user device).

[0018] A “payment device” may include any suitable device that may be used to conduct a financial transaction, such as to provide payment credentials to a merchant. The payment device may be a software object, a hardware object, or a physical object. As examples of physical objects, the payment device may comprise a substrate such as a paper or plastic card, and information that is printed, embossed, encoded, or otherwise included at or near a surface of an object. A hardware object can relate to circuitry (e.g., permanent voltage values), and a software object can relate to non-permanent data stored on a device. A payment device may be associated with a value such as a monetary value, a cryptocurrency amount, a discount, or store credit, and a payment device may be associated with an entity such as a bank, a merchant, a payment processing network, or a person. A payment device may be used to make a payment transaction. Suitable payment devices can be hand-held and compact so that they can fit into a user's wallet and/or pocket (e.g., pocket-sized). Example payment devices may include smart cards, magnetic stripe cards, keychain devices (such as the Speedpass™ commercially available from Exxon-Mobil Corp.), etc. If the payment device is in the form of a debit, credit, or smartcard, the payment device may also optionally have features such as magnetic stripes. Such devices can operate in either a contact or contactless mode. In some embodiments, a mobile device can function as a payment device (e.g., a mobile device can store and be able to transmit payment credentials for a transaction).

[0019] A “credential” may be any suitable information that serves as reliable evidence of worth, ownership, identity, or authority. A credential may be a string of numbers, letters, or any other suitable characters that may be present or contained in any object or document that can serve as confirmation.

25 **[0020]** A “value credential” may be information associated with worth. Examples of value credentials include payment credentials, coupon identifiers, information needed to obtain a promotional offer, etc.

[0021] “Payment credentials” may include any suitable information associated with an account (e.g., a payment account and/or payment device associated with the account). Such information may be directly related to the account or may be derived from information related to the account. Examples of account information may include a PAN (primary account number or “account number”), username, expiration date, CVV (card verification value), dCVV (dynamic card verification value), CVV2 (card verification value 2), CVC3 card verification values, etc. CVV2 is generally understood to be a static

verification value associated with a payment device. CVV2 values are generally visible to a user (e.g., a consumer), whereas CVV and dCVV values are typically embedded in memory or authorization request messages and are not readily known to the user (although they are known to the issuer and payment processors). Payment credentials
5 may be any information that identifies or is associated with a payment account. Payment credentials may be provided in order to make a payment from a payment account. Payment credentials can also include a username, an expiration date, a gift card number or code, and any other suitable information.

[0022] An "application" may be computer code or other data stored on a
10 computer readable medium (e.g., memory element or secure element) that may be executable by a processor to complete a task.

[0023] A "resource provider" may be an entity that can provide a resource such as goods, services, information, and/or access. Examples of a resource provider includes merchants, access devices, secure data access points, etc. A "merchant" may
15 typically be an entity that engages in transactions and can sell goods or services, or provide access to goods or services.

[0024] An "acquirer" may typically be a business entity (e.g., a commercial bank) that has a business relationship with a particular merchant or other entity. Some entities can perform both issuer and acquirer functions. Some embodiments may encompass
20 such single entity issuer-acquirers. An acquirer may operate an acquirer computer, which can also be generically referred to as a "transport computer."

[0025] An "authorizing entity" may be an entity that authorizes a request. Examples of an authorizing entity may be an issuer, a governmental agency, a document repository, an access administrator, etc. An "issuer" may typically refer to a
25 business entity (e.g., a bank) that maintains an account for a user. An issuer may also issue payment credentials stored on a user device, such as a cellular telephone, smart card, tablet, or laptop to the consumer.

[0026] A "digital wallet" may contain electronic information for conducting transactions. A digital wallet may store user profile information, payment credentials,
30 bank account information, cryptocurrency account information, one or more digital wallet identifiers and/or the like and can be used in a variety of transactions, such as but not limited to eCommerce, social networks, money transfer/ personal payments, mobile commerce, proximity payments, gaming, and/or the like for retail purchases, digital

goods purchases, utility payments, purchasing games or gaming credits from gaming websites, transferring funds between users, and/or the like. A digital wallet may be designed to streamline the purchase and payment process. A digital wallet may allow the user to load one or more payment cards onto the digital wallet so as to make a
5 payment without having to enter an account number or present a physical card.

[0027] A “digital wallet provider” may include an entity, such as an issuing bank or cryptocurrency exchange, which issues a digital wallet to a user that enables the user to conduct financial transactions. A digital wallet provider may provide standalone user-facing software applications that store account numbers on behalf of a cardholder (or
10 other user) to facilitate payments at more than one unrelated merchant, perform person-to-person payments, or load financial value into the digital wallet. A digital wallet provider may enable a user to access its account via a personal computer, mobile device or access device. Additionally, a digital wallet provider may also provide one or more of the following functions: storing one or more payment cards, maintaining one or
15 more cryptocurrency accounts, storing other information including billing address, shipping addresses, and transaction history, initiating a transaction by one or more methods, such as providing a username and password, NFC or a physical token, and may facilitate pass-through or two-step transactions.

[0028] An “exchange” may be an entity that facilitates exchanges of
20 cryptocurrency and fiat currency between parties. The exchange may manage any suitable number of accounts associated with registered parties. Users that want to sell cryptocurrency may conduct a cryptocurrency transaction to transfer their cryptocurrency to the exchange and the exchange may manage the cryptocurrency on behalf of the user. Users may additionally, or alternatively, transfer fiat currency to the
25 exchange and the exchange may manage the users’ fiat currency within the exchange. A user may provide the exchange a “buy request” indicating that the user wishes to purchase a particular amount of cryptocurrency for a particular amount (or within a range of the particular amount) of fiat currency. Users may also provide the exchange a
30 “sell request” indicating that the user wishes to sell cryptocurrency for a particular amount (or within a range of the particular amount) of fiat currency. The exchange may be configured to match a buy requests to a sell request in order to identify a buyer that is willing to purchase cryptocurrency at the fiat currency amount (or within the range) at which the seller is interested in selling. If a match is found, the exchange can facilitate a transfer of the fiat currency from the buyer’s account within the exchange to the seller’s

account within the exchange. The exchange can also facilitate the transfer of the cryptocurrency from the seller's account within the exchange to the buyer's account within the exchange.

[0029] A "cryptocurrency network" may include a one or more computers that participate in maintaining a cryptocurrency ledger. In some cryptocurrency networks, the distributed cryptocurrency ledger may comprise a blockchain. A "blockchain" is a decentralized and distributed digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the collusion of the network. Examples of a cryptocurrency network may include networks of computers that manage any suitable cryptocurrency including, but not limited to, Bitcoin, Litecoin, Ethereum, Zcash, Dash, Ripple, and Monero.

[0030] A "server computer" may include a powerful computer or cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a Web server. The server computer may be coupled to a database and may include any hardware, software, other logic, or combination of the preceding for servicing the requests from one or more client computers. The server computer may comprise one or more computational apparatuses and may use any of a variety of computing structures, arrangements, and compilations for servicing the requests from one or more client computers.

[0031] As noted above, in certain circumstances, it is desirable to transfer value in one form of currency from one person to another person in another form of currency. For example, it can be desirable to send a cryptocurrency amount to a second user using fiat currency held by a first user. Such transfers, however, can take a significant amount of time. For example, if the first user uses an account such as a demand account as a funds source, a transfer such as an ACH transfer can take one, two, or three days to complete. As such, it would be desirable to reduce the transaction time for a transaction that transfers one form of currency using another form of currency.

[0032] Embodiments of the invention address these and other problems. In embodiments of the invention, a first user operating a first user device may wish to transfer value to a second user operating a second user device. The first user may wish to send funds in one currency (e.g., U.S. dollars) and the second user may wish to

receive the funds in a different currency (e.g., a cryptocurrency). The first user can provide an alias or a credential that are specifically associated with an account of the second user, and a transfer amount to the first authorizing entity computer after the first user authenticates themselves with the first authorization entity computer 104. Through
5 the authentication, the first authorization entity computer 104 can identify the account of the first user.

[0033] The first authorizing entity computer can then generate and then transmit a push transfer message comprising the credential and the amount to a second authorizing entity computer via a processing network computer. The credential can
10 include a PAN or primary account number (e.g., a 16 digit credit, debit, or stored value account number), and the push transfer message can be an OCT (original credit transaction) message. The second authorizing entity computer may be associated or hold an account of an exchange that operates an exchange computer such as a
15 cryptocurrency exchange computer. The second authorizing entity computer can then adjust a value of the account based on the amount in the push transfer message. For example, the second authorizing entity computer can manage a suspense account and the suspense account can be credited for the amount in the push transfer message.

[0034] In the method, the second authorizing entity computer also transmits a credit message comprising the credential and the amount to the exchange computer.
20 The cryptocurrency exchange computer then communicates with an alias directory computer to obtain an alias associated with credential. Once the alias associated with the push transfer message is identified by the exchange computer, the exchange computer then credits a cryptocurrency account associated with the alias of the second user in an amount of cryptocurrency corresponding to the amount in the push transfer
25 message. The crediting can be performed by communicating with a blockchain network that records the added cryptocurrency value to the cryptocurrency account of the second user.

[0035] At a later time, funds can be transferred from the account of the first user managed by first authorizing entity computer to the second authorizing entity computer
30 which holds the account of the exchange computer.

[0036] FIG. 1 shows a block diagram of a system and overlaid method. The method is for obtaining a cryptocurrency wallet and then obtaining a credential such as a PAN (e.g., a 16 digit PAN) for the wallet. Note that the credential in this instance can

be in the form of a credit or debit card number, but does not have an underlying credit or debit card account. Rather, the credential can be tied to a different type of account, such as a cryptocurrency account, where the cryptocurrency account has its own identifier. The cryptocurrency account identifier can be, for example, a public key of a public-private key pair, which can be linked to an alias such as a phone number.

[0037] The system includes a second user device 112 operated by a second user, where the second user device 112 is in communication with an exchange computer 110. In some embodiments, the second user device 112 can be a mobile device such as a mobile phone. The exchange computer 110 can be in communication with an alias directory computer 116. As will be explained in detail below, the alias directory computer 116 can issue a credential 150 such as a PAN. The second user device 112, the exchange computer 110, and the alias directory computer 116 can communicate via various APIs (application program interfaces).

[0038] The computers and devices in the system in FIG. 1 can be in operative communication with each other through any suitable communication channel or communications network. Suitable communications networks may be any one and/or the combination of the following: a direct interconnection; the Internet; a Local Area Network (LAN); a Metropolitan Area Network (MAN); an Operating Missions as Nodes on the Internet (OMNI); a secured custom connection; a Wide Area Network (WAN); a wireless network (e.g., employing protocols such as, but not limited to a Wireless Application Protocol (WAP), I-mode, and/or the like); and/or the like. Messages between the computers, networks, and devices may be transmitted using a secure communications protocols such as, but not limited to, File Transfer Protocol (FTP); HyperText Transfer Protocol (HTTP); Secure Hypertext Transfer Protocol (HTTPS), Secure Socket Layer (SSL), ISO (e.g., ISO 8583) and/or the like.

[0039] In step S10, a second user using the second user device 112 may wish to obtain a cryptocurrency wallet from an exchange operating the exchange computer 110. The second user can initiate a registration process by downloading or accessing a base application provided by the exchange computer 110, and then providing the exchange computer 110 with personal information and supporting KYC (know your customer) documents using the second user device 112 (e.g., via the application). After the exchange computer 110 this information, the exchange computer 110 can validate the second user by performing a risk analysis, KYC screening and sanction screening. If the risk analysis and the screening processes are successful, then the exchange computer

110 can create and store a user profile for the second user, and can issue a wallet such as a cryptocurrency wallet (e.g., a blockchain wallet) to the second user operating the second user device 112. In the creation of the cryptocurrency wallet, the exchange computer 110 can initiate the generation of a public-private key pair that is specifically associated with the second user and the second user device 112. In some embodiments, the public key can be used to identify the cryptocurrency wallet and the private key can be used to sign data for transactions conducted using the cryptocurrency wallet. The exchange computer 110 can then determine an alias for the cryptocurrency wallet. The alias can be any suitable information that can be used to identify the cryptocurrency wallet. Examples of aliases can include e-mail addresses, phone numbers, public keys of public-private key pairs, passwords, randomly created user identifiers, etc.

[0040] In step S12, after the exchange computer 110 determines the alias, the exchange computer transmits the alias of the second user to the alias directory computer 116.

[0041] After receiving the alias, the alias directory computer 116 can create a credential 150 for the second user. In some embodiments, the credential 150 can be a primary account number that is 16 digits long and can have the form of a debit or credit card number. The credential 150 that is created by the alias directory computer 116 can be stored in association with the alias in a database at the alias directory computer 116.

[0042] In step S16, the alias directory computer 116 transmits the credential to the exchange computer 110, which assigns it to the second user's blockchain wallet. In other embodiments, the alias directory computer 116 can transmit the credential directly to the second user device 112.

[0043] In step S18, the exchange computer 110 then provides the wallet details including the credential, the alias for the cryptocurrency wallet, and the wallet private key (e.g., used to conduct cryptocurrency transactions) to the second user device 112 of the second user. The alias, the credential and the wallet private key may be stored in a secure memory in the second user device 112. In some embodiments, the exchange computer 110 may store the private key for the second user and can function as a custodian and can conduct transactions using the private key on behalf of the second user. In some embodiments, the exchange computer 110 can delete the credential that

was created by the alias directory computer 116, so that it only stores the alias and the second user's underlying information in a database.

5 [0044] Once the second user operating the second user device 112 is registered with the exchange computer 110, the second user device 112 can perform transactions using the credential.

[0045] FIG. 2 shows a block diagram of a system and overlaid method for performing a transaction according to an embodiment of the invention. The system includes a first user device 102 that is communication with a first authorizing entity computer 104. The first user device 102 can be operated by a first user, and the first
10 authorizing entity computer 104 can be a computer that is operated by an issuer, which holds an account of first user. The first user device can communicate with a processing network computer 106, which may be turn be in communication with a processing network computer 106. The second authorizing entity computer 108 can be in communication with an exchange computer 110. The exchange computer 110 can be in
15 communication with a blockchain network 114 and an alias directory computer 116. The exchange computer 110 can be in communication with a second user device 112, and may manage a digital wallet application on the second user device 112.

[0046] The computers and devices in the system in FIG. 1 can be in operative communication with each other through any suitable communication channel or
20 communications network. Suitable communications networks may be any one and/or the combination of the following: a direct interconnection; the Internet; a Local Area Network (LAN); a Metropolitan Area Network (MAN); an Operating Missions as Nodes on the Internet (OMNI); a secured custom connection; a Wide Area Network (WAN); a wireless network (e.g., employing protocols such as, but not limited to a Wireless
25 Application Protocol (WAP), I-mode, and/or the like); and/or the like. Messages between the computers, networks, and devices may be transmitted using a secure communications protocols such as, but not limited to, File Transfer Protocol (FTP); HyperText Transfer Protocol (HTTP); Secure Hypertext Transfer Protocol (HTTPS), Secure Socket Layer (SSL), ISO (e.g., ISO 8583) and/or the like.

30 [0047] In some embodiments, the communication paths and routing between the first authorizing entity computer 104, the processing network computer 106, and the second authorizing entity computer 108 can correspond to a traditional credit and debit card processing network. The computers in the processing network can communicate

using a protocol such as ISO 8583. Communications of the other computers and devices between each other or with the first authorizing entity computer 104, the processing network computer 106, and/or the second authorizing entity computer 108 can use a different communication protocol such as one using HTTPS.

5 **[0048]** The first user device 102 and the second user device 112 can be computational devices such as laptop computers or mobile phones. Additional descriptions of exemplary user devices and user device features are described above and below.

10 **[0049]** The first authorizing entity computer 104 and the second authorizing entity computer 108 can be operated by first and second authorizing entities, respectively. The first authorizing entity computer 104 can manage an account of the first user operating the first user device 102. The second authorizing entity computer 108 can operate various accounts including a suspense account (alternatively referred to as a settlement account), and an account of the exchange that operates the exchange
15 computer 110. In some embodiments, the first authorizing entity operating the first authorizing entity computer 104 can be a first issuer that holds a credit, debit, or stored value account for the first user. The second authorizing entity can be a second issuer that holds a credit, debit, or stored value account for the exchange operating the exchange computer 110.

20 **[0050]** The processing network computer 106 may be disposed between (in an operational sense) the first authorizing entity computer 104 and the second authorizing entity computer 108. The processing network computer 106 may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. For
25 example, the processing network computer 106 may comprise a server coupled to a network interface (e.g., by an external communication interface), and databases of information. The processing network computer 106 may be representative of a payment processing network. An exemplary payment processing network may include VisaNet™. Payment processing networks such as VisaNet™ are able to process credit card
30 transactions, debit card transactions, and other types of commercial transactions. VisaNet™, in particular, includes a VIP system (Visa Integrated Payments system) which processes authorization requests and a Base II system which performs clearing and settlement services. The processing network computer 140 may use any suitable wired or wireless network, including the Internet.

[0051] The blockchain network 114 may include any suitable subsystems and/or networks used to manage blockchain services. The blockchain network 160 may further include a plurality of nodes, such that at least one node is an initiator node. In embodiments, initiator node may be a node associated with the mobile wallet application on the second user device 112. Responsive to receiving a cryptocurrency transaction from the second user device 112 of the second user, the initiator node may validate and propagate the cryptocurrency transaction to other nodes of the blockchain network 160.

[0052] The exchange computer 110 can facilitate the exchange of different types of currency (e.g., fiat currency to cryptocurrency and vice-versa). Further details regarding the exchange computer 110 are provided below.

[0053] The alias directory computer 116 can store aliases for cryptocurrency accounts and credentials corresponding to those cryptocurrency accounts. Further details regarding the alias directory computer 116 can be found in further detail below.

[0054] Methods according to embodiments of the invention can be described with reference to FIG. 2.

[0055] The method begins with a first user operating the first user device 102 expressing an intent to pay a second user operating the second user device 112. However, the first user may wish to transfer value using fiat currency and the second user may receive the value in cryptocurrency. The second user may provide the first user and/or the first user device 102 the credential that received by the first user device 102 in the process described above with respect to FIG. 1. The second user may alternatively provide the first user and/or the first user device 102 the alias that was issued in the process described above with respect to FIG. 1.

[0056] In step S20, using an application such as a wallet application on the first user device 102, the first user device 102 can enter the credential of the second user or the alias thereof into the first user device 102 along with an amount to transfer. In some embodiments, the wallet application may be one that is managed by the first authorizing entity computer 104. This transaction information is then then transmitted to the first authorizing entity computer 104.

[0057] In step S22, after receiving the transaction information, the first authorizing entity computer 104 can generate a push transfer message comprising at least the transfer amount and the credential and can transmit it to the processing network

computer 106. If the first authorizing entity computer received the alias from the second user operating the second user device 112 instead of the credential, then the first authorizing entity computer 104 can provide the alias to the alias directory computer 116. The alias directory computer 116 can then look up the corresponding credential, and then can transmit it back to the first authorizing entity computer 104. In other embodiments, if the first authorizing entity computer 104 receive the credential such as a primary account number from the first user device 102, then the first authorizing entity computer 104 can generate the push transfer message using the received credential.

[0058] In some embodiments, the push transfer instruction message can be an original credit transaction (OCT) transfer message and may comprise at least the credential associated with the receiver and the transfer amount. An OCT (Original Credit Transaction) can be a clearing and settlement credit transaction designed for use in business applications such as a business money transfer or business-to-consumer repayments. The OCT can be a transaction used to deliver funds to the receiver account. It is separate from, and can take place after, an AFT transaction in some cases. This timing is to ensure that payment funds are secured before funds are sent to the receiver.

[0059] In step S24, after receiving the push transfer message, the processing network computer 106 can analyze the credential and determine that the push transfer message should be routed to the second authorizing entity computer 108. In some embodiments, the credential can have a first portion (e.g., the first six digits) that can identify the second authorizing entity computer 108, and it can be used to route the push transfer message to the correct authorizing entity computer. The processing network computer 106 can then transmit the push transfer message to the second authorizing entity computer 108.

[0060] In step S26, after the second authorizing entity computer 108 receives the push transfer message, the second authorizing entity computer 108 can analyze the push transfer message and perform additional processing. For example, the second authorizing entity computer 108 can adjust (e.g., credit) an amount associated with an account, such as a suspense account (or a settlement account) for the amount in the push transfer message. The suspense account can aggregate amounts of transfer or payments to and from different users, such that the funds can be used in settlement processes between various authorizing entity computers or transport computers (e.g., acquirer computers). The second authorizing entity computer 108 can then transmit the

details of the push transfer message to the exchange computer 110 in a credit message. As noted above, in some embodiments, the exchange computer 110 can have a separate account for the exchange computer 110 and the second authorizing entity computer 108 can transfer funds from the suspense account to the exchange computer account as appropriate.

[0061] In step S28, after receiving the details of the push transfer message, the second authorizing entity computer 108 can transmit the credential to the alias directory computer 116. The alias directory computer 116 can then use the credential to look up the alias that corresponds to the credential. The alias directory computer 116 can then transmit the retrieved alias to the exchange computer 110.

[0062] In step S30, after receiving the alias corresponding to the credential, the exchange computer 110 can look up the cryptocurrency account associated with the second user operating the second user device 112 using the alias. If the alias is a phone number or an e-mail address, the exchange computer 110 can look up a corresponding public/private key pair associated with the cryptocurrency wallet held by the second user device 112 to provide the appropriate credit to the second user's cryptocurrency account.

[0063] In step S30, once the exchange computer 110 has identified the cryptocurrency account and the transfer amount, the exchange computer 110 can communicate with the blockchain network 114 to initiate the transfer of an amount of cryptocurrency equivalent to the amount in the push transfer message from an exchange computer cryptocurrency account to the cryptocurrency account of the second user operating the second user device 112. The blockchain network 114 can be a blockchain network such as a Bitcoin, Ethereum or the like, and can record the cryptocurrency amount by transferring the amount from a cryptocurrency account of the exchange computer to the cryptocurrency account of the second user operating the second user device 112.

[0064] In step S32, after the exchange computer 110 has initiated the transfer or credit of cryptocurrency to the cryptocurrency account of the second user operating the second user device 112, or after the exchange computer 110 has received a notification from the blockchain network 114 that the transfer has been completed, then a notification can be sent from the exchange computer 110 to the second user device 112 indicating that the second user has received the credit of cryptocurrency.

[0065] In some embodiments, at a later time, in step S34, a clearing and settlement process can occur between the first authorizing entity computer 104, the processing network computer 106, and the second authorizing entity computer 108. In the clearing and settlement process, actual settlement funds can be transferred
5 between the authorizing entity computers and any transport computers to settle transactions conducted by them. In this case, the first authorizing entity computer 104 can send a settlement amount to the second authorizing entity computer 108 via the processing network computer 106, and the funds can be held in the suspense account at the second authorizing entity computer 108 along with funds from other transfers of
10 value.

[0066] In step S36, after the second authorizing entity computer 108 receives the funds in the suspense account, actual funds in the transfer amount or another amount (e.g., the transfer amount less any fees allocated to the entities processing the transaction) can be transferred to the exchange computer 110. Alternatively, the second
15 authorizing entity computer 108 can hold a fiat currency account for the exchange computer 110 and the fiat currency funds can be transferred from the suspense account to the fiat currency account held by the second authorizing entity operating the second authorizing entity computer 108 on behalf of the exchange computer 110.

[0067] An example of the first user device 102 according to an embodiment of the invention is shown in FIG. 3. The components in the first user device 102 can also be in
20 the second user device 112 in FIG. 2. In some embodiments, first user device 102 may include circuitry that is used to enable certain device functions, such as telephony. The functional elements responsible for enabling those functions may include a processor 102B that can execute instructions that implement the functions and operations of the device. Processor 102B may access the memory 102F (or another suitable data storage
25 region or element) to retrieve instructions or data used in executing the instructions, such as provisioning scripts and mobile applications. Data input/output elements 102D, such as a keyboard or touchscreen, may be used to enable a user to operate the first user device 102 and input data. Data input/output elements may also be configured to
30 output data (via a speaker of the device, for example). Display 102C may also be used to output data to a user. Communications element 102E may be used to enable data transfer between the first user device 102 and a wired or wireless network (via antenna 102G, for example) to assist in connectivity to the Internet or other network, and enabling data transfer functions.

[0068] In some embodiments, first user device 102 may also include contactless element interface to enable data transfer between contactless element (not shown) and other elements of the device, where contactless element may include a secure memory and a near field communications data transfer element (or another form of short range communications technology). A cellular phone or similar device is an example of a first user device 102 that may be used in accordance with embodiments of the present invention. However, other forms or types of devices may be used without departing from the underlying concepts of the invention. For example, the first user device 102 may alternatively be in the form of a payment card, a key fob, a PDA, a tablet computer, a net book, a laptop computer, a smart watch, an automobile with remote capabilities, etc.

[0069] The memory 102F may comprise an application 102A and/or any other suitable module or data. The first user device 102 may have any number of mobile applications installed or stored on the memory 102F and is not limited to that shown in FIG. 2. The memory 102F may also comprise code, executable by the processor 102B for implementing the methods discussed herein.

[0070] The application 102A (e.g., a digital wallet application, a browser application, etc.) may be configured to render at least one user interface. The application 102A may, in some examples, be configured to access one or more Internet websites (e.g., associated with a cryptocurrency account, associated with an Issuer, etc.) to provide input and initiate, facilitate, and manage cryptocurrency account transactions.

[0071] An example of the exchange computer 110, according to an embodiment of the invention, is shown in FIG. 4. The exchange computer 110 may comprise a processor 110A, a network interface 110B, a database 110C, and a computer readable medium 110D. The database 110C can store user account information including public private key pairs, user personal information, aliases, etc.

[0072] The computer readable medium 110D may comprise a registration module 110E, an exchange module 110F, and a processing module 110G. The computer readable medium 110D may also comprise code, executable by the processor 110A for implementing the methods discussed herein. For example, the code can be executable by the processor 110A to perform a method comprising: receiving, from a second authorizing entity computer, a credit message comprising a credential and an amount, the amount being present in a push transfer message transmitted by a first authorizing

entity computer and comprising a credential and the amount; communicating with an alias directory computer to obtain an alias associated with credential; receiving the alias; and adjusting a cryptocurrency account associated with the alias in an amount of cryptocurrency corresponding to the amount in the push transfer message.

- 5 **[0073]** The registration module 110E may comprise code that, when executed, causes the processor 110A to receive registration information associated with an exchange user (e.g., an individual, an issuer, a cryptocurrency seller, etc.). The registration module 110E may cause the processor 110A to maintain an exchange account using the registration information. A record maintaining exchange account
10 information may be stored in the database 110C. For example, the record may indicate a cryptocurrency amount, a fiat currency amount, past transaction information, personal information of the user, etc.

- [0074]** The exchange module 110F may comprise code that, when executed, causes the processor 110A to provide a current exchange rate such as a
15 cryptocurrency exchange rate. For example, the processor 110A may be configured to receive a message indicating that a push transfer message with an amount of fiat currency was received for a second user. The exchange module 110F and the processor 110A can determine the equivalent amount of fiat currency to credit to a cryptocurrency account of the second user.

- 20 **[0075]** The exchange module 110F may also comprise code that, when executed, causes the processor 110A to receive a buy request message. In some examples, the buy request message is associated with a participant of the exchange. A buy request message may indicate an exchange identifier associated with a buyer, an amount of cryptocurrency to purchase, an amount of fiat currency to be exchanged for
25 cryptocurrency, an acceptable buy price/price range, or the like. Any suitable parameters may be included in the buy request message to facilitate a purchase of cryptocurrency for fiat currency.

- [0076]** The exchange module 110F may comprise code that, when executed, causes the processor 110A to receive a sell request message. In some examples, the
30 sell request message is associated with a participant of the exchange. The sell request message may indicate an exchange identifier associated with a seller, an amount of cryptocurrency to sell, an acceptable sale price/price range in fiat currency, or the like.

Any suitable parameters may be included in the sell request message to facilitate a sale of cryptocurrency for fiat currency.

[0077] The exchange module 110F may comprise code that, when executed by the processor 110A, performs operations comprising matching a buy request to a sell request of one or more users of the exchange. If a matching sell request is found, the exchange module 110F may facilitate a transfer of cryptocurrency from the seller's exchange account to an exchange account of the buyer and a transfer of fiat currency from the buyer's exchange account to an exchange account of the seller. The exchange module 110F may comprise code that, when executed, causes the processor 110A to transmit a buy response message. The buy response message may indicate a successful exchange of fiat currency for cryptocurrency or that the exchange was unsuccessful.

[0078] The processing module 110G may comprise code that, when executed, causes the processor 110A to perform transaction processing such as transmitting messages to various cryptocurrency blockchains to record credits to various users, and to adjust internal ledgers that keep track of amounts received from the users and amounts owed to the users.

[0079] An example of the authorizing entity computer 120, according to an embodiment of the invention, is shown in FIG. 6. The authorizing entity computer 120 may comprise a processor 120A, a network interface 120B, a database 120C, and a computer readable medium 120D. The database 120C may hold data for one or more suspense accounts as well as individual user accounts. The components in the authorizing entity computer 120 can be in the first authorizing entity computer 104 or the second authorizing entity computer 108 in FIG. 2.

[0080] The computer readable medium 120D may comprise a management module 120E, a transaction module 120F, an exchange module 120G, and a settlement module 120H. The computer readable medium 120D may also comprise code, executable by the processor 120A for implementing the methods discussed herein. For example, the computer readable medium 120D can include code, executable by the processor 120A for performing a method comprising: a method comprising: receiving, from a first authorizing entity computer, a push transfer message comprising a credential and an amount; adjusting a value of an account based on the amount in the push transfer message; and transmitting, to a cryptocurrency exchange computer, a

credit message comprising the credential and the amount, wherein the cryptocurrency exchange computer communicates with an alias directory computer to obtain an alias associated with credential, and then credits a cryptocurrency account associated with the alias in an amount of cryptocurrency corresponding to the amount in the push transfer message

[0081] The management module 120E may comprise code that, when executed, cause the processor 120A to issue and/or manage a payment account and associated payment devices for users.

[0082] The transaction module 120F may comprise code that, when executed, causes the processor 120A to process and/or authorize transactions. Before authorizing a transaction, the transaction module 120F may authenticate payment credentials received in the authorization request message, and credit funds in an associated payment account.

[0083] The exchange module 120G may comprise code that, when executed, causes the processor 120A to communicate with an exchange computer.

[0084] The settlement module 120H may comprise code, that, when executed causes the processor 120A to perform clearing and settlement processing.

[0085] As discussed above, the transaction processing system may utilize a blockchain network 114 comprising a blockchain. FIG. 6 shows block entries of an exemplary blockchain within the blockchain network 114, in accordance with one embodiment of the invention.

[0086] FIG. 6 shows a blockchain comprising block entries for at least a block A, a block B, and a block C. The blockchain may also include additional block entries before a block A and/or after a block C, which are not depicted in the figure.

[0087] Each block entry may comprise a header, a digital signature, a nonce, and information about a set of transactions. In some embodiments, each block entry may additionally include information from a previous block entry and/or be appended to a hash of a previous block entry, such that each block entry is connected with a plurality of previous block entries.

[0088] Referring to block A 600, header 601 may be a hash value that is unique to the block A, such that neither block B nor block C share a same header as block A. In some embodiments, header 601 may be a hash of information from block A, information

from a previous block, and/or any other suitable information (e.g., such as a timestamp, a Merkle tree root, etc.). Still referring to block A, a digital signature 602 may represent a hash of a previous block entry. In some embodiments, digital signature 602 may be a header of the previous block entry.

5 **[0089]** Nonce 603 may be a randomly generated number that is determined by a node (e.g., a user or computer) within the blockchain network 114 in order to validate block A and then add block A to the blockchain. Addition of a new block entry to the blockchain occurs when a new nonce for that block entry is solved by another node within the blockchain network.

10 **[0090]** Block A further includes a list of transactions 604, which may comprise transaction data for a plurality of cryptocurrency transactions that have been verified by the blockchain network 160. List of transactions 604 may comprise a list of cryptocurrency transaction identifiers, where each cryptocurrency transaction identifier is further associated with transaction data such as a transaction amount, an
15 address of a transaction sender, and an address of a transaction recipient. In some embodiments, the list of transactions 604 may be hashed and merged to form a Merkle tree root. In some embodiments, the Merkle tree root can be used to generate header 601 .

[0091] When adding a new block entry, the blockchain retrieves transactions for a
20 new list of transactions for the block entry from a set of unconfirmed transactions 610 (e.g., referred to as a "mempool" in some cases). The set of unconfirmed transactions 610 may comprise transactions that have been validated but have not yet been added to a block entry. Responsive to receiving a new cryptocurrency transaction, one or more nodes within the blockchain network may validate a signature of the transaction and
25 then transmit the transaction to the set of unconfirmed transactions 610. The transaction may then later be added to a new block entry of the blockchain and removed from the set of unconfirmed transactions 610.

[0092] Embodiments of the invention have a number of technical advantages. As noted by the above examples, embodiments of the invention can utilize an existing
30 payments infrastructure to securely process payment transactions using cryptocurrencies. As such, the computer architecture allows for many cryptocurrencies to be used for payments at a resource provider, without the need to update existing access device hardware or software. Further, because an existing payments

infrastructure is used, embodiments of the invention can perform security and validation checks used in traditional payment transactions on currently unregulated cryptocurrency transactions. Embodiments of the invention also allow for users to send and receive funds in different currencies in real time or near real time.

- 5 **[0093]** Any of the software components or functions described in this application, may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C++ or Perl using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions, or commands on a computer readable medium, such as a random
- 10 access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a CD-ROM. Any such computer readable medium may reside on or within a single computational apparatus, and may be present on or within different computational apparatuses within a system or network.
- 15 **[0094]** The above description is illustrative and is not restrictive. Many variations of the invention may become apparent to those skilled in the art upon review of the disclosure. The scope of the invention can, therefore, be determined not with reference to the above description, but instead can be determined with reference to the pending claims along with their full scope or equivalents.
- 20 **[0095]** One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the invention.
- [0096]** A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.
- 25 **[0097]** All patents, patent applications, publications, and descriptions mentioned above are herein incorporated by reference in their entirety for all purposes. None is admitted to be prior art.

WHAT IS CLAIMED IS:

1. A method comprising:
receiving, by a second authorizing entity computer from a first authorizing entity computer, a push transfer message comprising a credential and an amount;
adjusting, by the second authorizing entity computer, a value of an account based on the amount in the push transfer message; and
transmitting, by the second authorizing entity computer to a cryptocurrency exchange computer, a credit message comprising the credential and the amount, wherein the cryptocurrency exchange computer communicates with an alias directory computer to obtain an alias associated with credential, and then credits a cryptocurrency account associated with the alias in an amount of cryptocurrency corresponding to the amount in the push transfer message.
2. The method of claim 1, wherein the account is a suspense account held by a second authorizing entity associated with the second authorizing entity computer.
3. The method of claim 1, wherein the amount is in fiat currency.
4. The method of claim 1, further comprising:
transferring, by the second authorizing entity computer, the amount or another amount based on the amount to the cryptocurrency exchange computer.
5. The method of claim 1, wherein the push transfer message is received by the second authorizing entity computer from the first authorizing entity computer via a processing network computer.
6. The method of claim 1, wherein the credential is a primary account number.
7. The method of claim 1, wherein the account is a suspense account which receives values from different authorizing entity computers and transport computers for settlement of transactions processed by the different authorizing entity computers and transport computers.

8. The method of claim 1, wherein adjusting, by the second authorizing entity computer, the value of the account based on the amount in the push transfer message, comprises crediting, by the second authorizing entity computer, the value of the account based on the amount in the push transfer message.

9. The method of claim 1, wherein the alias directory computer maintains mappings between aliases and credentials.

10. The method of claim 1, wherein the cryptocurrency computer credits the account associated with the alias by communicating with a blockchain network to record the amount of cryptocurrency to a blockchain maintained by the blockchain network.

11. The method of claim 1, wherein the push transfer message is initiated after the first authorizing entity computer receives a transfer instruction from a first user device operated by a first user to transfer the amount of cryptocurrency to a second user operating a second user device.

12. The method of claim 1, wherein the account is a suspense account, and the method further comprises:

receiving, by the suspense account associated with the second authorizing entity computer, funds associated with the amount in the push transfer message; and

transferring, by the second authorizing entity computer, the funds to an account of the cryptocurrency exchange computer.

13. The method of claim 12, wherein the account of the cryptocurrency exchange computer is managed by the second authorizing entity computer.

14. The method of claim 12, wherein the account of the cryptocurrency exchange computer is managed by the cryptocurrency exchange computer or an entity associated with the cryptocurrency exchange computer.

15. A second authorizing entity computer comprising:

a processor; and
a non-transitory computer readable medium, the non-transitory computer readable medium comprising code, executable by the processor, for performing a method comprising:
receiving, from a first authorizing entity computer, a push transfer message comprising a credential and an amount;
adjusting a value of an account based on the amount in the push transfer message; and
transmitting, to a cryptocurrency exchange computer, a credit message comprising the credential and the amount, wherein the cryptocurrency exchange computer communicates with an alias directory computer to obtain an alias associated with credential, and then credits a cryptocurrency account associated with the alias in an amount of cryptocurrency corresponding to the amount in the push transfer message.

16. A method comprising:
receiving, by an exchange computer from a second authorizing entity computer, a credit message comprising a credential and an amount, the amount being present in a push transfer message transmitted by a first authorizing entity computer and comprising a credential and the amount;
communicating, by the exchange computer with an alias directory computer to obtain an alias associated with credential;
receiving, by the exchange computer, the alias; and
adjusting, by the exchange computer, a cryptocurrency account associated with the alias in an amount of cryptocurrency corresponding to the amount in the push transfer message.

17. The method of claim 16, wherein the exchange computer is a cryptocurrency exchange computer.

18. The method of claim 16, wherein the credential is a primary account number.

19. The method of claim 16, further comprising:

receiving funds associated with the amount in the push transfer message from the second authorizing entity computer.

20. The method of claim 19, wherein the funds are fiat currency funds.