

PUSH TRANSFER TO BLOCKCHAIN SYSTEM

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] This application is a PCT application which claims priority to U.S. Provisional Application No. 63/619,618, filed on January 10, 2024, which is herein
5 incorporated by reference in its entirety for all purposes.

BACKGROUND

[0002] A push transfer interaction involves pushing a value from a sender record to a receiver record associated with a receiver. The receiver can immediately utilize the value without waiting for subsequent finalization processing to take place.
10 However, push interactions such as these typically only utilize one type of value (e.g., a fiat value). As a result, the application of such push transfer interactions is limited in scope. In addition, the records associated with the users conducting such push transactions are not transparent or immutable. As such, the records associated with such conventional records can potentially be subject to possible unauthorized
15 manipulation or hacking.

[0003] It would be desirable to provide for a system and method that allows conventional push interactions to be used with other types of value such that they have a wider range of use. It would also be desirable to provide for a system and a method that allows such push transactions to be conducted using records that
20 are transparent and immutable.

[0004] Embodiments of the invention address these and other problems individually and collectively.

SUMMARY

[0005] One embodiment includes a method comprising: receiving, by a network
25 processing computer from a sending entity computer, a push transfer message for a push transfer, the push transfer message comprising a receiver address associated with a record of a receiver and a value; validating, by the network processing

computer, the push transfer message; and transmitting, by the network processing computer to an aggregator computer, the push transfer message, wherein the aggregator computer thereafter initiates a recordation of a transfer the value from an aggregator address associated with the aggregator computer to the receiver address
5 on a blockchain managed by a blockchain network.

[0006] Another embodiment of the invention includes a network processing computer comprising: a processor; and a non-transitory computer readable medium comprising code, executable by the processor, for performing operations comprising: receiving, from a sending entity computer, a push transfer message for a push transfer,
10 the push transfer message comprising a receiver address associated with a record of a receiver and a value; validating the push transfer message; and transmitting, to an aggregator computer, the push transfer message, wherein the aggregator computer thereafter initiates a recordation of a transfer the value from an aggregator address associated with the aggregator computer to the receiver address on a blockchain

[0007] Another embodiment of the invention includes a method comprising: receiving, by an aggregator computer from a network processing computer, a push transfer message comprising a receiver address associated with a record of receiver and a value; transmitting, by the aggregator computer to a node in a blockchain network managing a blockchain, a recordation request comprising an aggregator
20 address associated with the aggregator computer to the receiver address; and receiving, by the aggregator computer from the node in the blockchain network, a recordation response indicating that the value was recorded on the blockchain.

[0008] Another embodiment of the invention includes an aggregator computer. The aggregator computer comprises: a processor, and a non-transitory computer
25 readable medium. The non-transitory computer readable medium comprises code, executable by the processor for performing operations comprising: receiving, from a network processing computer, a push transfer message comprising a receiver address associated with a record of receiver and a value; transmitting, to a node in a blockchain network managing a blockchain, a recordation request comprising an aggregator
30 address associated with the aggregator computer to the receiver address; and

receiving, from the node in the blockchain network, a recordation response indicating that the value was recorded on the blockchain.

[0009] These and other embodiments are described in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

5 **[0010]** FIG. 1. shows a block diagram and an interaction flow according to an embodiment of the invention.

[0011] FIG. 2 shows a portion of a diagram of a blockchain.

[0012] FIG. 3 shows a block diagram of a network processing computer.

[0013] FIG. 4 shows a block diagram of an aggregator computer.

10 **[0014]** FIG. 5 shows a block diagram of a user device.

DETAILED DESCRIPTION

[0015] Prior to discussing specific embodiments of the invention, some discussion of some terms may be helpful.

15 **[0016]** An “alias” may be nickname associated with a real identifier. An alias can be a phone number, e-mail address, username, etc. associated with a user’s real name (e.g., John Smith). An alias can have any suitable number of type of characters. An alias can be used to conduct transfers instead of sensitive information. This preserves privacy and data security.

20 **[0017]** A “user” may include an individual or other entity that can use something. Examples of users can include natural persons, and organizations such as ride sharing organizations, insurance claim processing organizations, etc. In some embodiments, a user may be associated with one or more personal accounts and/or mobile devices. The user may also be referred to as a cardholder, account holder, or consumer in some embodiments. A user may be a “receiver” that can receive something. A user
25 can also be a “sender,” which is someone that can send something.

[0018] A “receiving entity” can be an entity that receives something, typically on behalf of a receiver. The receiving entity can manage a record (e.g., an account) of a

receiver. Examples of receiving entities can include authorizing entities such as issuers, acquirers, service providers etc. A receiving entity can operate a receiving entity computer.

[0019] A “sending entity” can be an entity that sends something, typically on behalf of a sender. The sending entity can manage a record (e.g., an account) of a sender. Examples of sending entities can include authorizing entities such as issuers, acquirers, digital wallet providers (e.g., cryptocurrency wallet providers), service providers etc. A sending entity can operate a sending entity computer. In some cases, the sending entity computer can be an application server, which supports an application running on a user device.

[0020] 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.

[0021] An “issuer” may typically refer to a 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.

[0022] 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.

[0023] A “transfer application” can include an application facilitating the transfer of funds between multiple parties. For instance, a transfer application can include a peer-to-peer transaction application. The transfer application can be executed on a

mobile device associated with a user, and the transfer application can be implemented using a server (e.g., an application server) in communication with the mobile device. The transfer application can provide an account (e.g., from a digital wallet which may be part of the transfer application or external to it) for each user. The transfer
5 application can allow a user to select a recipient user to transfer a specified amount of funds to the recipient user. The transfer application can then transfer the specified amount from an account for the user to an account for the recipient user.

[0024] An “application server” can be a server computer that is specifically designed to run applications. For instance, an application server can perform
10 processing tasks relating to the above-described transfer application, such as provide user account details to be displayed on the transfer application executing on the mobile device or facilitate transfer of funds between users on the transfer application.

[0025] A “push transfer message” can include a message that causes value (e.g., funds) to be pushed from one entity to another. In some embodiments, for
15 example, a push transaction message can be generated by an application server to initiate a transaction between a sender and a receiver to push funds to the receiver. In a push transaction, the funds transfer messaging is not initiated by the intended recipient of the funds. The push transfer message can include user account details, a credential, an address, and/or an alias relating to the receiver, a transaction amount,
20 and a push transfer indicator (e.g., an OCT indicator). In some instances, the push transfer message can comprise an original credit transaction (OCT) format. Push transactions such as those that use OCT (original credit transaction) messages are processed as single-message transactions with authorization and clearing performed as a single step. This means that once an authorizing entity computer approves the
25 push transfer message, they can make the funds immediately available to a recipient record, or recipient account, instead of waiting for a separate clearing instruction. Consequently, the push transfer transactions are non-reversible because once value is made available, the recipient can use the value immediately.

[0026] An “interaction” can be a reciprocal action, effect, or influence.
30 An interaction, for example, could be an exchange or transaction between two or more parties. An example of an interaction is a transaction.

[0027] A “transaction” may be an action or exchange between two or more parties. For example, a transaction may include a first entity requesting resources from a second entity. In this example, the transaction is completed when the resources are either provided to the first entity or the transaction is declined. In another example, a
5 transaction can include an interaction where a receiver pushes value to a receiver address.

[0028] A “node” may include an intersection point. In some embodiments, a node may be a physical electronic device that is capable of creating, receiving, or transmitting data. In other embodiments, a node may be a software module on a
10 computing device, the software module a connection point in a communication network. In some embodiments, a node may be a computing device within an asset transfer network. A node may be able to mint an asset, transfer an asset, receive an asset, validate an asset, maintain a ledger of transactions, and/or perform any other suitable functions.

[0029] A “record” may refer to evidence of a data element. A digital record can be electronic documentation of a data element. A record can include a record identifier and record information. For example, record information can include information a data element (e.g., a digital asset) and/or information about the data element (e.g., a digital signature associated with the digital asset). A record identifier can be a number, title,
20 or other value used for identifying a record. A record can also be an account, which records a balance. An account identifier can be an example of a record identifier. Examples of records include medical records, academic records, transaction records within a ledger of transactions, etc.

[0030] “Account information” may include any suitable information associated
25 with an account (e.g., a personal account number 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”), an address, username, expiration date, and verification values such as CVV, dCVV, CVV2, dCVV2, and CVC3
30 values.

[0031] A “ledger of transactions” may include a compilation of data from previous transactions. The ledger of transactions may be a database or other comparable file structure that may be configured to store data from all previous digital asset transfers, including the date and time of the transfer, the transfer amount, and identification information for the participants of the transfer (e.g., the sender and the receiver of the transfer amount). In some embodiments, the ledger of transactions may be in the form of an electronic ledger (e.g., blockchain) in which data already stored in the electronic ledger is unalterable. In some embodiments, each node within an asset transfer network may store their own copy of the ledger of transactions. In other embodiments, only some nodes store their own copy of the ledger of transactions. In further embodiments, some nodes may have a restricted view of the ledger of transactions. For example, some nodes may only be able to view and/or verify transactions to which they were a party.

[0032] A ledger of transactions may include transaction records that are digitally signed (e.g., with a private key) in order to protect the transaction entries in the ledger from being doctored with false transaction data. This can prevent double spending and make all transactions immutable and irreversible, and therefore make the ledger trustworthy.

[0033] In some embodiments, a ledger of transactions can be publicly viewable. For example, one or more entities may have access to the ledger, and may be able to consult the ledger to determine whether a certain transaction actually took place, or whether a certain value is authentic. In some embodiments, the ledger may only be partially viewable to one or more entities.

[0034] As used herein, a “blockchain” may comprise a series of blocks. Each block in the blockchain may include an electronic record of one or more historical transactions, as well as metadata. In some embodiments, blocks in the blockchain can be linked by including a reference to the previous block (e.g., a hash output of a previous block). Each new block in the blockchain may be algorithmically determined based on new transactions and previous blocks in the blockchain. As a result, any tampering of data stored in these previous blocks can be detected.

[0035] A block can include both a “block body” and a “block header.” The block header can be a block identifier or label. The block header can serve to identify the block, and block headers can be used to link blocks together. The block body can include the information stored in the block. For example, record information stored in
5 a block can be considered the block body. The block body can also include other data, such as reference to a previous block (e.g., a previous block header), a timestamp, a random number, a hash of record information (e.g., transaction data), and/or any other suitable information. In some embodiments, the block body can be all block data besides the block header. A block header can be created based on the block body.
10 For example, some or all of the block body information can be used as inputs in a hashing algorithm, encrypted, or otherwise manipulated to create a block header. A previous block can be linked to a current block by using the previous block header as in input when generating the current block header.

[0036] A “cryptocurrency transaction” can be a payment transaction that utilizes
15 a cryptocurrency instead of fiat currency. Cryptocurrency transactions may include (but are not limited to) transactions using Bitcoin, Ethereum, and USDC. Cryptocurrency transactions may further be processed by a blockchain network. Responsive to processing, cryptocurrency transactions may be added to a ledger of transactions included within the blockchain network.

20 **[0037]** An “address” can be data which identifies a particular location. The location can be a location in a data structure, a destination, or the like. An example of an address can be a public key of a public-private key pair. The address can be used as an identifier for a particular user or device.

[0038] A “cryptocurrency address” can be an identifier that indicates a
25 destination and/or a source for a cryptocurrency payment. For example, a cryptocurrency address may be a string of at least 26 to 35 alphanumeric characters. As another example, a cryptocurrency address may be a public key. Each cryptocurrency transaction may include a cryptocurrency address of a source of a cryptocurrency payment, and a cryptocurrency address of a recipient (e.g., a
30 destination of a cryptocurrency payment).

[0039] FIG. 1 shows system 10 and a process flow according to an embodiment. The system can include a sender user device 100 in communication with a sending entity computer 102. The sending entity computer 102 is in communication with a network processing computer 104. The network processing computer 104 is in communication with an aggregator computer 108. The aggregator computer 108 can be in communication with a blockchain network 110 which manages a blockchain 110A, and a receiving entity computer 112. A receiver user device 114 operated by a receiver can be in communication with the receiving entity computer 112.

[0040] A sender (not shown) can be an individual user that operates the sender user device 100 and can have a sender record that is managed by the sending entity computer 102. The sending entity computer 102 can be operated by a sending such as a digital wallet, an issuer (e.g., an issuing bank) or an acquirer (e.g., an acquiring bank). The sender record can be an account such as a debit account, a credit account, or a stored value account. The sender record can have one type of value, such as amounts in fiat currency.

[0041] A receiver (not shown) can also be an individual user. The receiver can operate the receiver user device 114 and can have a receiver record that is managed by the receiving entity computer 140. The receiving entity computer 140 can be operated by a receiving entity such as a digital wallet provider (e.g., a cryptocurrency wallet provider). The receiver record can maintain one or more values of a different type than the sender record. For example, the receiver record can be a digital value account such as a cryptocurrency account.

[0042] Although a user (e.g., the sender, the receiver, etc.) that is an individual is discussed as an example, other types of users can include organizations such as ride sharing organizations, insurance claim processing organizations, etc.

[0043] In some embodiments, the sender user device 100 and the receiver user device 114 can each have transfer applications such as digital wallet applications on them. The transfer applications can be managed by different application servers, which may be part of or separate from the sending entity computer 102 and the receiving entity computer 112.

[0044] The network processing computer 104 can be in a transaction processing network or system, which may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, transaction scoring services, and clearing and settlement services. An exemplary transaction processing system may include VisaNet™. Transaction processing systems such as VisaNet™ are able to process credit card transactions, debit card transactions, and other types of commercial transactions. VisaNet™, in particular, may include a VIP system (Visa Integrated Payments system) which processes authorization requests and a Base II system which performs clearing and settlement services.

[0045] The blockchain network 110 can comprise a plurality of nodes, where each of the nodes includes a blockchain. The nodes can operate using a proof of work of consensus process to validate blocks of transactions before incorporating them onto the blockchain 110A.

[0046] The aggregator computer 108 can be programmed to perform functions such as receiving a push transfer messages, validating the push transfer messages, initiating recordation of interactions on the blockchain 110A managed by the blockchain network 110, and performing notification and settlement processing.

[0047] In some embodiments, the sending entity computer 102 and the aggregator computer 108 can communicate with the network processing computer 104 via one or more secure APIs.

[0048] Messages between the devices in FIG. 1 can 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), SSL, ISO (e.g., ISO 8583) and/or the like. The communications network that may include 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. The communications network can use any suitable communications

protocol to generate one or more secure communication channels. A communications channel may, in some instances, comprise a secure communication channel, which may be established in any known manner, such as through the use of mutual authentication and a session key, and establishment of a Secure Socket Layer (SSL) session.

[0049] Methods according to embodiments of the invention can be described with respect to FIG. 1. In FIG. 1, the sending entity computer 102 may operate on behalf of a sender operating the sender user device 100. The sender may wish to transfer a second type of value to a receiver operating the receiver user device 114.

10 The sender, however, may use a first type of value when sending the second type of value to the receiver. The second type of value may be recorded on the blockchain 110A by the blockchain network 110. For example, the sender may wish to pay the receiver by sending an amount of cryptocurrency (USDC or US digital currency) to a receiver record using an amount of fiat currency (e.g., a US dollars) in a sender record.

15 In some embodiments, the sending entity computer 102 can be operated by a sending entity such as an issuing bank that holds an account such as a credit or debit card account of the sender.

[0050] Prior to step S2, the sender may enter information into a transfer application on the sender user device 100 operated by the sender to express an intent to push a value to a receiver record of the receiver. The sender user device 100 may have a list of options such as transferring value from or to any combination of records including fiat currency accounts (e.g., debit, credit, and stored value accounts) and blockchain accounts (e.g., cryptocurrency accounts). The information can include an address, alias or identifier for the receiver operating the receiver device, a second type of value to transfer to the receiver record of the receiver, and a first type of value that will be used to conduct the interaction. In some embodiments, the first type of value may be a fiat currency (e.g., 100 U.S. dollars) and the second type of value may be a blockchain value such as a cryptocurrency value (e.g., 100 US digital currency). The sending user device 100 can generate and transmit a push origination message with this information to the sending entity computer 102.

[0051] In step S2, the sending entity computer 102 receives the push origination message comprising at least a second type of value, and a receiver address, a receiver identifier, or an alias associated with the receiver address from the sender user device 100. The sending entity computer 102 can parse the push origination message, and then format a push transfer message from the data in the push origination message.

[0052] In step S4, after receiving the push origination message from the sender user device 100, the sending entity computer 102 sends the push transfer message for the push transfer to the network processing computer 104. In some embodiments, a secure API can be used as an interface between the sending entity computer 102 and the network processing computer 104 when sending the push transfer message. As noted above, the push transfer message can comprise a receiver address associated with a record of the receiver operating the receiver user device 114 (or an alias or an identifier associated with the receiver address), and the value. In some embodiments, the push transfer message is an original credit transaction message (OCT message) and the receiver address is a crypto wallet address (e.g., a public key of a public/private key pair) associated with a cryptocurrency account of the receiver. In other embodiments, the push transfer message comprises an alias. The network processing computer 104 can search a database and can retrieve the receiver address using the alias. The database can contain a receiver address to alias mapping. It may also contain alias to credential (e.g., primary account number) mappings. In some embodiments, the push transfer message can also include a storage application (e.g., a wallet application) ID such as a crypto wallet ID. The storage application wallet ID and the receiver address may be the same or different data. In some embodiments, there may be additional information that can be collected by the sending entity computer 102 such as the sender's name, the sender's physical address, the receiver's name, the receiver's physical address, the receiver's country, a time and date of transaction, a transaction identifier, etc. In some embodiments, the network processing computer 104 can validate all of this information provided by the sending entity computer 102 before continuing to process the push transfer message.

[0053] At step S6, assuming that the information from the sending entity computer 102 is validated, the network processing computer 104 sends the push

transfer message comprising at least the receiver address and the value to the aggregator computer 108. In some embodiments, the aggregator computer 108 and the network processing computer 104 can communicate via a secure API. The aggregator computer 108 can validate the data in the push transfer message. For
5 example, the aggregator computer 108 can determine if the receiver address is a valid address on the blockchain 110A before initiating recordation of the value on the blockchain 110A. After validating the data, the sending entity computer 102 can initiate a recordation of a transfer the value from an aggregator address associated with the aggregator computer to the receiver address on a blockchain managed by a
10 blockchain network.

[0054] In step S8, after validating the push transfer message, the aggregator computer 108 can generate and transmit a recordation request message comprising at least the receiver address and the amount to the blockchain network 110 which manages the blockchain 110A. The nodes in the blockchain network 110 can then
15 proceed to record the transaction to transfer the amount from an aggregator computer address to the receiver address on the blockchain 110A. The blockchain network 110 can inform the aggregator computer 108 once the recordation of the transaction on the blockchain 110A is completed. Blockchain recordation protocols such as those used in Bitcoin or Ethereum can be used to record the transaction on the blockchain
20 110A.

[0055] Current blockchain technologies, such as Bitcoin and Ethereum, maintain an append-only ledger in a network. The ledger includes a list of blocks of transaction data, the blocks are cryptographically chained together as depicted in FIG. 2. A block can be created using a computationally intensive process called proof-of-
25 work in which valid blocks need to demonstrate a sufficient "difficulty" (i.e., sufficient computation power to create on average). Proof-of-work blockchains are secured and can be verified by nodes racing to be the first to solve a math puzzle. The nodes that solve the puzzle are "miners," which can receive a reward for solving the puzzle before other nodes solve the puzzle. In a proof of stake system, staking serves a similar
30 function to proof of work's mining, in that it's the process by which a network participant gets selected to add the latest batch of transactions to the blockchain and earn some crypto in exchange. The exact details vary by project, but in general proof of stake

blockchains employ a network of “validators” who contribute — or “stake” — their own crypto in exchange for a chance of getting to validate new transaction, update the blockchain, and earn a reward.

5 **[0056]** In step S10, after the recordation of the transaction on the blockchain 110A by the blockchain network 110 is completed, the aggregator computer 108, can transmit a notification to the receiving entity computer 112 with an indication that the value has been transferred to the receiver’s address.

10 **[0057]** In step S12, the receiving entity computer 112 can transmit a message to the receiver user device 114 of the receiver indicating that the value has been transferred to the receiver’s address.

15 **[0058]** In other aspects of the invention, the network processing computer 104 has settlement accounts which can receive fiat funds from the sending entity computer 102, and then transfer them to the aggregator computer 108 (or an account managed by the aggregator computer 108). At a later time, the transfer of fiat funds associated with the transaction can be sent from the sending entity computer 102 to the aggregator computer 108 via the network processing computer 104. The network processing computer 104 can keep a record of various transactions conducted using the sending entity computer 102 and other sending entity computers with the aggregator computer 108, and can receive fiat funds for those transactions and transfer them to the aggregator computer 108.

20 **[0059]** FIG. 2 shows a diagram of a portion of a blockchain, which can be used in embodiments of the invention. The blockchain 200 can comprise a plurality of blocks, for example, block 202A and block 202B. Each block can comprise a block header, e.g., block 202A comprises block header 204. The block header 204 can include multiple data elements, such as a previous header hash 206 and a Merkle root 208. The previous header hash 206 can be a hash of the previous block’s header. The Merkle root 208 can be a root of a Merkle tree, which is a tree in which every leaf node is labelled with the hash of a data block, for example, data in a transaction 210-214. Each leaf of the Merkle tree can represent one of the transactions 210-214. Although a certain number of blocks and transactions are show in FIG. 2 for purposes of

illustration, blockchains according to embodiments can have any suitable number of transactions or blocks.

[0060] FIG. 3 shows a block diagram of a network processing computer 300 according to embodiments. The exemplary network processing computer 300 may comprise a processor 304. The processor 304 may be coupled to a memory 302, a network interface 306 and a computer readable medium 308. The computer readable medium 308 can comprise a push transfer module 308A, a validation module 308B, a settlement module 308C, and a record management module 308D, an alias resolution module 308E, and a communication module 308F.

[0061] The memory 302 can be used to store data and code. The memory 302 may be coupled to the processor 304 internally or externally (e.g., cloud based data storage), and may comprise any combination of volatile and/or non-volatile memory, such as RAM, DRAM, ROM, flash, or any other suitable memory device. For example, the memory 302 can store interaction data, receiver addresses, tokens, aliases, credentials, etc.

[0062] The computer readable medium 308 may comprise code, executable by the processor 304, for performing a method comprising: receiving, from a sending entity computer, a push transfer message for a push transfer, the push transfer message comprising a receiver address associated with a record of a receiver and a value; validating the push transfer message; and transmitting, to an aggregator computer, the push transfer message, wherein the aggregator computer thereafter initiates a recordation of a transfer the value from an aggregator address associated with the aggregator computer to the receiver address on a blockchain.

[0063] The push transfer module 308A can include code, executable by the processor 304 for processing push transfer transactions. Such processing can include re-formatting push transfer messages, and routing push transfer messages to the appropriate aggregator computers.

[0064] The validation module 308B can include code, executable by the processor 304, for validating transactions. As noted above, validation can include

checking to see if the push transfer messages contain appropriate data and are being sent from legitimate senders to legitimate receivers.

[0065] The settlement module 308C can include code, executable by the processor 304, for performing settlement processes. Such settlement processes can include receiving fiat funds from sending entity computers and transmitting such fiat funds to aggregator computers.

[0066] The record management module 308D may comprise code or software, executable by the processor 304, for performing record management functions.

[0067] The alias resolution module 308E can include code, executable by the processor 304 for obtaining addresses (receiver or sender addresses such as cryptocurrency addresses) or credentials associated with aliases, and obtaining aliases associated with addresses or credentials.

[0068] The communication module 308F may comprise code or software, executable by the processor 304, for communicating with other devices. The communication module 308F may be configured or programmed to perform some or all of the functionality associated with receiving, sending, and generating electronic messages for transmission.

[0069] The network interface 306 may include an interface that can allow the network processing computer 300 to communicate with external computers. The network interface 306 may allow for communication of data to and from another device. Some examples of the network interface 306 may include a modem, a physical network interface (such as an Ethernet card or other Network Interface Card (NIC)), a virtual network interface, a communications port, a Personal Computer Memory Card International Association (PCMCIA) slot and card, or the like. The wireless protocols enabled by the network interface 306 may include Wi-Fi™. Data transferred via the network interface 306 may be in the form of signals which may be electrical, electromagnetic, optical, or any other signal capable of being received by the external communications interface (collectively referred to as “electronic signals” or “electronic messages”). These electronic messages that may comprise data or instructions may be provided between the network interface 306 and other devices via a

communications path or channel. As noted above, any suitable communication path or channel may be used such as, for instance, a wire or cable, fiber optics, a telephone line, a cellular link, a radio frequency (RF) link, a WAN or LAN network, the Internet, or any other suitable medium.

5 **[0070]** FIG. 4 shows a block diagram of an aggregator computer 400 according to embodiments. The aggregator computer 400 may comprise a processor 402. The processor 402 may be coupled to a memory 404, a network interface 406, and a computer readable medium 408. The network interface 406 can have the same or different characteristics as the network interface 306.

10 **[0071]** The memory 404 can be used to store data and code. In some embodiments, the memory 404 may be linked to a database 410. The memory 404 and/or the database 410 may be coupled to the processor 402 internally or externally (e.g., via cloud-based data storage), and may comprise any combination of volatile and/or non-volatile memory such as RAM, DRAM, ROM, flash, or any other suitable
15 memory device.

[0072] The computer readable medium 408 may comprise code, executable by the processor 402, for a method comprising: receiving, from a network processing computer, a push transfer message comprising a receiver address associated with a record of receiver and a value; transmitting, to a node in a blockchain network
20 managing a blockchain, a recordation request comprising an aggregator address associated with the aggregator computer to the receiver address; and receiving, from the node in the blockchain network, a recordation response indicating that the value was recorded on the blockchain.

[0073] The computer readable medium 408 may comprise several software
25 modules including, but not limited to, a blockchain interaction module 408A, a validation module 408B, a settlement module 408C, and a communication module 408D.

[0074] The blockchain interaction module 408A can include code, executable by the processor 402 to transmit messages to one or more blockchain networks and
30 receive messages from one or more blockchain networks. The messages may relate

to recording interactions on the blockchains managed by the one or more blockchain networks.

5 **[0075]** The validation module 408B can include code, executable by the processor 402 to validate interaction requests or requests to record interactions on blockchain networks.

[0076] The settlement module 408C may comprise code that causes the processor 402 to perform settlement processing with the network processing computer.

10 **[0077]** The communication module 408D may comprise code that causes the processor 402 to generate messages, forward messages, receive message, reformat messages, and/or otherwise communicate with other entities.

[0078] FIG. 5 shows a block diagram of a user device 500 according to embodiments. The user device 500 may comprise a processor 502. The processor 502 may be coupled to an input element 503, an output element 505, a memory 504, a network interface 506, and a computer readable medium 508. The computer readable medium 508 may comprise any suitable number and types of software modules. The network interface 506 can have the same or different characteristics as the network interface 306.

20 **[0079]** Examples of input elements may include microphones, keypads, touchscreens, sensors, etc. Examples of output elements may include speakers, display screens, and tactile devices. The processor 502 can be implemented as one or more integrated circuits (e.g., one or more single core or multicore microprocessors and/or microcontrollers) and can be used to control the operation of the user device 500. The processor 202 can execute a variety of programs in response to program code or computer-readable code and can maintain multiple concurrently executing programs or processes.

25 **[0080]** The memory 504 may be used to store data and code. The memory 504 may be coupled to the processor 502 internally or externally (e.g., via cloud-based data storage), and may comprise any combination of volatile and/or non-volatile

memory such as RAM, DRAM, ROM, flash, or any other suitable memory device. In some embodiments, the memory 504 may store the data items of a payload.

5 **[0081]** The computer readable medium 508 may comprise several software modules including, but not limited to, a transfer application 508A, an authentication module 508B, and a communication module 508C.

[0082] The transfer application 508A may enable communication with a transfer application server. The transfer application 508A may include instructions or code implementing a transfer application 508A for initiating a transfer of funds to a receiver account of a receiver.

10 **[0083]** The authentication module 508B can comprise code that causes the processor 502 to perform authentication processes including password verification, biometric verification, etc.

[0084] The communication module 508C may comprise code that causes the processor 502 to generate messages, forward messages, receive message, reformat
15 messages, and/or otherwise communicate with other entities.

[0085] Embodiments of the invention provide several technical advantages. For example, embodiments of the invention allow senders to push one type of value to a receiver that receives another type of value.

20 **[0086]** Another advantage is that the record of the value received by the receiver can be immutable and transparent, and is not subject to change by unauthorized means.

[0087] Another advantage is that embodiments of the invention can perform a number of validation steps, such as the validation for wallets across blockchains. This is particularly unique and advantageous in the environment of push transfer
25 transactions.

[0088] Further, the use of various APIs to communicate across the system requires the ability to configure cryptocurrency wallet elements. This is different than typical transactions because cryptocurrency uses unique addresses that must be formatted. In an embodiment of the present invention, the aggregator computer would

be able to receive a cryptocurrency wallet address and format the message to be used to complete the transaction and send cryptocurrency to the receiver.

[0089] 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, C++, C#, Objective-C, Swift, or scripting language such as Perl or Python 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 for storage and/or transmission, suitable media include random 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 compact disk (CD) or DVD (digital versatile disk), flash memory, and the like. The computer readable medium may be any combination of such storage or transmission devices.

[0090] Such programs may also be encoded and transmitted using carrier signals adapted for transmission via wired, optical, and/or wireless networks conforming to a variety of protocols, including the Internet. As such, a computer readable medium according to an embodiment of the present invention may be created using a data signal encoded with such programs. Computer readable media encoded with the program code may be packaged with a compatible device or provided separately from other devices (e.g., via Internet download). Any such computer readable medium may reside on or within a single computer product (e.g., a hard drive, a CD, or an entire computer system), and may be present on or within different computer products within a system or network. A computer system may include a monitor, printer, or other suitable display for providing any of the results mentioned herein to a user.

[0091] The above description is illustrative and is not restrictive. Many variations of the invention will become apparent to those skilled in the art upon review of the disclosure. The scope of the invention should, therefore, be determined not with reference to the above description, but instead should be determined with reference to the pending claims along with their full scope or equivalents.

[0092] 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.

[0093] As used herein, the use of "a," "an," or "the" is intended to mean "at least one," unless specifically indicated to the contrary.

5

WHAT IS CLAIMS IS:

1. A method comprising:
receiving, by a network processing computer from a sending entity computer, a push transfer message for a push transfer, the push transfer message comprising a receiver address associated with a record of a receiver and a value;
validating, by the network processing computer, the push transfer message; and
transmitting, by the network processing computer to an aggregator computer, the push transfer message, wherein the aggregator computer thereafter initiates a recordation of a transfer the value from an aggregator address associated with the aggregator computer to the receiver address on a blockchain managed by a blockchain network.
2. The method of claim 1, wherein the aggregator address is a public key associated with the aggregator computer.
3. The method of claim 1, wherein the receiver address is a public key associated with a private key of the receiver.
4. The method of claim 1, wherein the sending entity computer and the network processing computer communicate via an API.
5. The method of claim 1, wherein validating the push transfer message comprises validating that the receiver address is a valid address.
6. The method of claim 1, wherein the push transfer message is an OCT message.
7. The method of claim 1, further comprising:
receiving, by the network processing computer, a finalization value associated with the push transfer; and

transmitting, by the network processing computer, the finalization value to the aggregator computer.

8. The method of claim 1, wherein prior to receiving the push transfer message, the sending entity computer receives a push origination message comprising the value from a sender user device associated with a sender.

9. The method of claim 8, wherein the sender user device is a mobile phone.

10. The method of claim 1, wherein prior to receiving the push transfer message, the sending entity computer receives a push origination message from a sender user device associated with a sender, the push origination message comprising the value and a receiver alias.

11. The method of claim 10, wherein the push transfer message further comprises the receiver alias, and wherein the method further comprises:
resolving, by the network processing computer, the receiver alias into the receiver address.

12. A network processing computer comprising:
a processor; and
a non-transitory computer readable medium comprising code,
executable by the processor, for performing operations comprising:
receiving, from a sending entity computer, a push transfer message for a push transfer, the push transfer message comprising a receiver address associated with a record of a receiver and a value;
validating the push transfer message; and
transmitting, to an aggregator computer, the push transfer message,
wherein the aggregator computer thereafter initiates a recordation of a transfer the value from an aggregator address associated with the aggregator computer to the receiver address on a blockchain.

13. The network processing computer of claim 12, wherein in the operations, prior to receiving the push transfer message, the sending entity computer receives a push origination message from a sender user device associated with a sender, the push origination message comprising the value and a receiver alias.

14. The network processing computer of claim 13, wherein the push transfer message further comprises the receiver alias, and wherein the operations further comprise:

resolving the receiver alias into the receiver address.

15. A method comprising:

receiving, by an aggregator computer from a network processing computer, a push transfer message comprising a receiver address associated with a record of receiver and a value;

transmitting, by the aggregator computer to a node in a blockchain network managing a blockchain, a recordation request comprising an aggregator address associated with the aggregator computer to the receiver address; and

receiving, by the aggregator computer from the node in the blockchain network, a recordation response indicating that the value was recorded on the blockchain.

16. The method of claim 15, further comprising:

transmitting, by the aggregator computer, an interaction completion message to a storage application provider computer, the storage application provider computer holding a receiver record for the receiver.

17. The method of claim 15, further comprising:

receiving, by the aggregator computer from the network processing computer, a finalization value.

18. The method of claim 15, wherein the receiver address is a receiver public key of a receiver public-private key pair.
19. The method of claim 15, wherein the aggregator address is an aggregator public key or an aggregator public-private key pair.
20. The method of claim 15, wherein the push transfer message is an OCT message.