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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
02 January 2025 (02.01.2025)

WIPO | PCT

(10) International Publication Number
WO 2025/006457 A1

(51) International Patent Classification:
H04L 9/00 (2006.01) *H04L 9/32* (2006.01)

(21) International Application Number:
PCT/US2024/035400

(22) International Filing Date:
25 June 2024 (25.06.2024)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
63/511,543 30 June 2023 (30.06.2023) US

(71) Applicant: **VISA INTERNATIONAL SERVICE ASSOCIATION** [US/US]; P.O. Box 8999, San Francisco, California 94128 (US).

(72) Inventors: **SOOKIKIAN, Alex**; P.O. Box 8999, San Francisco, California 94128 (US). **JURSS, Bryce**; P.O. Box 8999, San Francisco, California 94128 (US).

(74) Agent: **JEWIK, Patrick** et al.; 1100 Peachtree Street, NE Suite 2800, Atlanta, Georgia 30309 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH,

(54) **Title:** BLOCKCHAIN INTERACTION METHOD USING TOKEN OR CREDENTIAL

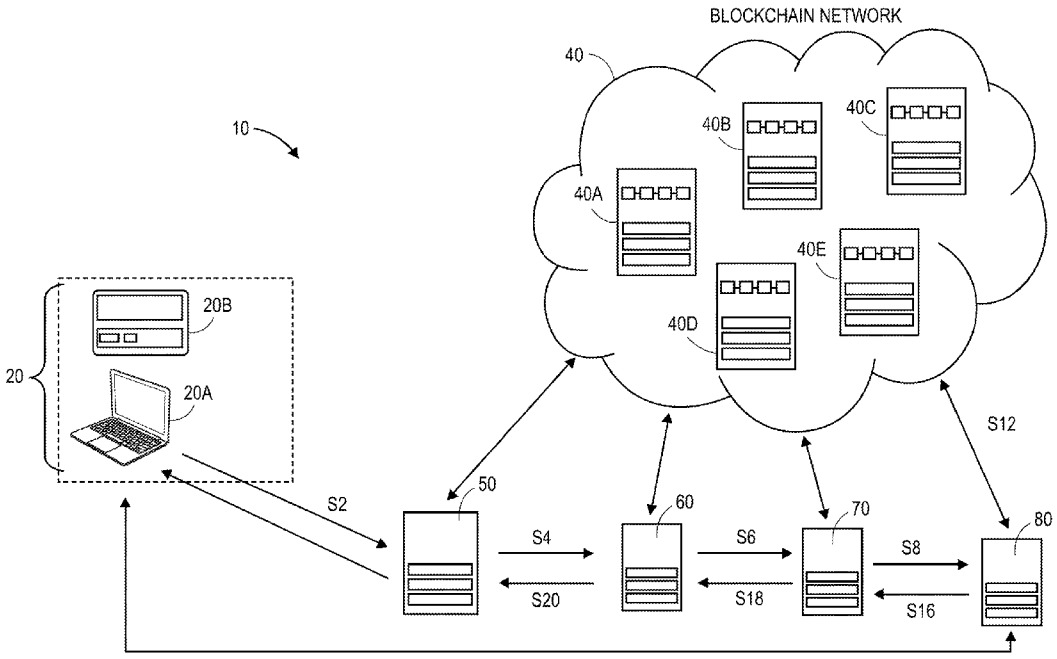

FIG. 1

(57) **Abstract:** A method is disclosed. It includes receiving, by a processing network computer, an authorization request message. The authorization request message comprises an amount and a credential or a token associated with a user as part of an interaction with a resource provider. The processing network computer transmits, to an authorizing entity computer, the authorization request message, which determines a first blockchain address associated with the user using the credential, and initiates a first blockchain transaction on a blockchain. The method also includes transmitting to the authorizing entity computer a post-authorization request message associated with the authorization request message. The authorizing entity computer initiates a second blockchain transaction transferring a first post-authorization amount associated with the amount from a second blockchain address to a third blockchain address associated with the processing network computer. The processing network computer provides a second post-authorization amount to a transport computer.

WO 2025/006457 A1

[Continued on next page]

TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

— *with international search report (Art. 21(3))*

BLOCKCHAIN INTERACTION METHOD USING TOKEN OR CREDENTIAL

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is a PCT application, which claims priority to U.S. Provisional Application No. 63/511,543, filed on June 30, 2023, which is herein incorporated by reference in its entirety.

BACKGROUND

[0002] Blockchain transactions such as cryptocurrency transactions have gained popularity in recent years, and their use is expected to grow over time. However, their adoption for use mainstream transactions has been slow. One of the barriers for adoption relates to the speed of transactions. For example, as noted above, an Ethereum transaction can take 1-10 minutes to complete depending upon the number of required confirmations, while a Bitcoin transaction can take between 1-1.5 hours to complete.

[0003] Conventional blockchain transaction such as cryptocurrency transactions are “push” transactions which are initiated by the sender. As such, conventional blockchain transactions have limited security mechanisms such as fraud detection capabilities. In addition, such transactions are often de-centralized and unregulated. As such, the conventional blockchain transactions lack the security required to provide confidence to very large groups of users.

[0004] Lastly, blockchain transactions are often limited to the type of value provided by a particular blockchain, and are inflexible in this regard. That is, typical blockchain transactions involve the transfer of one type of value to another person that receives the same type of value.

[0005] Embodiments of the invention address these and other problems, individually and collectively.

BRIEF SUMMARY

[0006] One embodiment includes a method comprising: receiving, by a processing network computer, an authorization request message for a transaction, the authorization request message comprising an amount and a credential or a token associated with a user as part of an interaction with a resource provider; transmitting, by the processing network computer to an authorizing entity computer, the authorization request message comprising the credential, wherein the authorizing entity computer determines a first blockchain address associated with the user using the credential, and initiates a first blockchain transaction of the amount or a derivative thereof on a blockchain managed by a blockchain network from the first blockchain address associated with the user to a second blockchain address associated with the authorizing entity computer; transmitting, by the processing network computer, to the authorizing entity computer a post-authorization request message associated with the transaction, wherein the authorizing entity computer initiates a second blockchain transaction transferring a first post-authorization amount associated with the amount from the second blockchain address to a third blockchain address associated with the processing network computer; and providing, by the processing network computer, a second post-authorization amount including the amount to a transport computer associated with the resource provider.

[0007] Another embodiment of the invention includes a processing network computer comprising: a processor; and a non-transitory computer readable medium, the non-transitory computer readable medium comprising code, executable by the processor, to perform operations comprising: receiving an authorization request message for a transaction, the authorization request message comprising an amount and a credential or a token associated with a user as part of an interaction with a resource provider; transmitting, to an authorizing entity computer, the authorization request message comprising the credential, wherein the authorizing entity computer determines a first blockchain address associated with the user using the credential, and initiates a first blockchain transaction of the amount or a derivative thereof on a blockchain managed by a blockchain network from the first blockchain address associated with the user to a second blockchain address associated with the authorizing entity computer; transmitting to the authorizing entity computer a post-authorization request message associated with the transaction, wherein the authorizing entity computer initiates a second blockchain transaction transferring a first

post-authorization amount associated with the amount from the second blockchain address to a third blockchain address associated with the processing network computer; and providing a second post-authorization amount including the amount to a transport computer associated with the resource provider.

[0008] Another embodiment includes a method comprising: receiving, by an authorizing entity computer from a processing network computer, an authorization request message comprising an amount and a credential associated with a user as part of a transaction between a resource provider and the user; determining a first blockchain address associated with the user using the credential; initiating a first blockchain transaction of the amount or a derivative thereof on a blockchain managed by a blockchain network from the first blockchain address associated with the user to a second blockchain address associated with the authorizing entity computer; receiving, by the authorizing entity computer from the processing network computer, a post-authorization request message associated with the transaction; and initiating, by the authorizing entity computer, a second blockchain transaction transferring a first post-authorization amount associated with the amount from the second blockchain address to a third blockchain address associated with the processing network computer, wherein the processing network computer provides a second post-authorization amount including the amount to a transport computer associated with the resource provider.

[0009] Another embodiment of the invention includes an authorizing entity computer comprising: a processor; and a computer readable medium coupled to the processor. The computer readable medium comprises code, executable by the processor for implementing operations. The operations comprise: receiving, by an authorizing entity computer from a processing network computer, an authorization request message comprising an amount and a credential associated with a user as part of a transaction between a resource provider and the user; determining a first blockchain address associated with the user using the credential; initiating a first blockchain transaction of the amount or a derivative thereof on a blockchain managed by a blockchain network from the first blockchain address associated with the user to a second blockchain address associated with the authorizing entity computer; receiving, by the authorizing entity computer from the processing network computer, a post-authorization request message associated with the transaction; and initiating,

by the authorizing entity computer, a second blockchain transaction transferring a first post-authorization amount associated with the amount from the second blockchain address to a third blockchain address associated with the processing network computer, wherein the processing network computer provides a second post-authorization amount including the amount to a transport computer associated with the resource provider.

[0010] These and other embodiments of the invention are described in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] FIG. 1 shows a block diagram of a system according to an embodiment, with an overlaid authorization process flow.

[0012] FIG. 2 shows a flow diagram illustrating a clearing process according to embodiments.

[0013] FIG. 3 shows a flow diagram illustrating a settlement process according to embodiments.

[0014] FIG. 4 shows a block diagram of an examplary user device acording to embodiments.

[0015] FIG. 5 shows a block diagram of an examplary node computer according to embodiments.

[0016] FIG. 6 shows a block diagram of an examplary authorizing entity computer according to embodiments.

[0017] FIG. 7 shows a block diagram of an examplary processing network computer according to embodiments.

[0018] FIG. 8 shows a diagram illustrating a portion of a blockchain according to some embodiments.

TERMS

[0019] Before discussing specific embodiments of the invention, some descriptions of some terms may be helpful.

[0020] A “key” may include a piece of information that is used in a cryptographic algorithm to transform input data into another representation. A cryptographic algorithm can be an encryption algorithm that transforms original data into an alternate representation, or a decryption algorithm that transforms encrypted information back to the original data. Examples of cryptographic algorithms may include triple data encryption standard (TDES), data encryption standard (DES), advanced encryption standard (AES), etc.

[0021] A "public key" may include an encryption key that may be shared openly and publicly. The public key may be designed to be shared and may be configured such that any information encrypted with the public key may only be decrypted using a private key associated with the public key (i.e., a public/private key pair).

[0022] A "private key" may include any encryption key that may be protected and secure. A private key may be securely stored at an entity and may be used to decrypt any information that has been encrypted with an associated public key of a public/private key pair associated with the private key.

[0023] A “public/private key pair” may refer to a pair of linked cryptographic keys generated by an entity. The public key may be used for public functions such as encrypting a message to send to the entity or for verifying a digital signature which was supposedly made by the entity. The private key, on the other hand may be used for private functions such as decrypting a received message or applying a digital signature. In some embodiments, the public key may be authorized by a body known as a Certification Authority (CA) which stores the public key in a database and distributes it to any other entity which requests it. The private key can typically be kept in a secure storage medium and will usually only be known to the entity. Public and private keys may be in any suitable format, including those based on Rivest-Shamir-Adleman (RSA) or elliptic curve cryptography (ECC).

[0024] 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 authorizing entity may operate an authorizing entity computer. An “issuer” may refer to a business entity (e.g., a bank) that issues and optionally 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.

[0025] A “resource provider” may be an entity that can provide a resource such as goods, services, information, and/or access to a location (e.g., a parking space, a transit terminal, etc.). Examples of resource providers include merchants, governmental authorities, secure data providers, etc. A resource provider may operate one or more access devices.

[0026] 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 such single entity issuer-acquirers. An acquirer may operate an acquirer computer, which can also be generically referred to as a “transport computer.”

[0027] A “communication device” may comprise any suitable electronic device capable of remote electronic communication. Examples of remote communication capabilities include using a mobile phone (wireless) network, wireless data network (*e.g.*, 3G, 4G or similar networks), Wi-Fi, Bluetooth, Bluetooth Low Energy (BLE), Wi-Max, or any other communication medium that may provide access to a network such as the Internet or a private network. Examples of communication devices include mobile phones (*e.g.*, cellular phones), PDAs, tablet computers, net books, laptop computers, wearable devices (e.g., watches), vehicles such as automobiles and motorcycles, personal music players, hand-held specialized readers, etc.

[0028] 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 also be referred to as a cardholder, account holder, or consumer in some embodiments.

[0029] A “user device” may be any suitable device that can interact with a user device (e.g., a payment card or mobile phone). User devices may be in any suitable form. Some examples of user devices include cellular phones, PDAs, personal computers (PCs), tablet computers, and the like. In some embodiments, where a user device is a mobile device, the mobile device may include a display, a memory, a processor, a computer-readable medium, and any other suitable component.

[0030] "Credentials" may comprise any evidence of authority, rights, or entitlement to privileges. For example, access credentials may comprise permissions to access certain tangible or intangible assets, such as a building or a file. Examples of credentials may include passwords, passcodes, or secret messages. In another example, payment credentials may include any suitable information associated with and/or identifying 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 an "account identifier" such as a PAN (primary account number or "account number"), a token, a subtoken, a gift card number or code, a prepaid card number or code, a user name, an expiration date, a CVV (card verification value), a dCVV (dynamic card verification value), a CVV2 (card verification value 2), a CVC3 card verification value, etc. An example of a PAN is a 16-digit number, such as "4147 0900 0000 1234". In some embodiments, credentials may be considered sensitive information.

[0031] A "token" may be a substitute value for a credential. A token may be a string of numbers, letters, or any other suitable characters. Examples of tokens include access tokens such as payment tokens, data that can be used to access secure systems or locations, etc.

[0032] A "payment token" may include an identifier for a payment account that is a substitute for an account identifier, such as a primary account number (PAN) and/or an expiration date. For example, a token may include a series of alphanumeric characters that may be used as a substitute for an original account identifier. For example, a token "4900 0000 0000 0001" may be used in place of a PAN "4147 0900 0000 1234." In some embodiments, a token may be "format preserving" and may have a numeric format that conforms to the account identifiers used in existing transaction processing networks (e.g., ISO 8583 financial transaction message format). In some embodiments, a token may be used in place of a PAN to initiate, authorize, settle or resolve a payment transaction or represent the original credential in other systems where the original credential would typically be provided. In some embodiments, a token value may be generated such that the recovery of the original PAN or other account identifier from the token value may not be computationally derived. Further,

in some embodiments, the token format may be configured to allow the entity receiving the token to identify it as a token and recognize the entity that issued the token.

[0033] "Tokenization" is a process by which sensitive data is replaced with substitute data. For example, a real credential (e.g., a primary account number (PAN)) may be tokenized by replacing the real account identifier with a substitute number that may be associated with the real credential. Further, tokenization can be applied to any other information to substitute the underlying information with a token. "Token exchange" or "de-tokenization" can be a process of restoring the data that was substituted during tokenization. For example, a token exchange may include replacing a payment token with its associated primary account number (PAN). Further, de-tokenization or token exchange may be applied to any other information to retrieve the substituted information from a token. In some embodiments, token exchange can be achieved via a transactional message, such as an ISO message, an application programming interface (API), or another type of web interface (e.g., web request).

[0034] A "token service computer" can include a system that that services tokens. In some embodiments, a token service computer can facilitate requesting, determining (e.g., generating) and/or issuing tokens, as well as maintaining an established mapping of tokens to primary account numbers (PANs) in a repository (e.g., token vault). In some embodiments, the token service computer may establish a token assurance level for a given token to indicate the confidence level of the token to PAN binding. The token service computer may include or be in communication with a token vault where the generated tokens are stored. The token service computer may support token processing of payment transactions submitted using tokens by de-tokenizing the token to obtain the actual PAN.

[0035] A "token domain" may indicate an area and/or circumstance in which a token can be used. Examples of the token domain may include, but are not limited to, payment channels (e.g., e-commerce, physical point of sale, etc.), POS entry modes (e.g., contactless, magnetic stripe, etc.), and merchant identifiers to uniquely identify where the token can be used. A set of parameters (i.e., token domain restriction controls) may be established as part of token issuance by the token service computer that may allow for enforcing appropriate usage of the token in payment transactions. For example, the token domain restriction controls may restrict the use of the token

with particular presentment modes, such as contactless or e-commerce presentment modes. In some embodiments, the token domain restriction controls may restrict the use of the token at a particular merchant that can be uniquely identified. Some exemplary token domain restriction controls may require the verification of the presence of a token cryptogram that is unique to a given transaction. In some embodiments, a token domain can be associated with a token requestor.

[0036] "Token expiry date" may refer to the expiration date/time of the token. The token expiry date may be passed among the entities of the tokenization ecosystem during transaction processing to ensure interoperability. The token expiration date may be a numeric value (e.g., a 4-digit numeric value). In some embodiments, the token expiry date can be expressed as a time duration as measured from the time of issuance.

[0037] A "contract address" may include a digital address that identifies a smart contract. A contract address can identify a smart contract on a blockchain. A contract address could also be a public key of a smart contract.

[0038] An "interaction application" can be an application that can allow for a user to perform an interaction with another entity. One example of an interaction application is a digital wallet or digital wallet application.

[0039] A "digital wallet" may contain electronic information for conducting transactions. A digital wallet may store user profile information, payment credentials, 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, cryptocurrency transactions, 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 payment without having to enter an account number or present a physical card.

[0040] A "blockchain" can be a distributed database that maintains a continuously growing list of records secured from tampering and revision. A blockchain

can be a non-fungible token blockchain, a cryptocurrency blockchain, or a combination thereof. A blockchain may include a number of blocks of interaction records. Each block in the blockchain can contain also include a timestamp and a link to a previous block. Stated differently, interaction records in a blockchain may be stored as a series of "blocks," or permanent files that include a record of a number of interactions occurring over a given period of time. Blocks may be appended to a blockchain by an appropriate node after it completes the block and the block is validated. Each block can be associated with a block header. In embodiments of the invention, a blockchain may be distributed, and a copy of the blockchain may be maintained at each full node in a verification network. Any node within the verification network may subsequently use the blockchain to verify interactions. A blockchain can be stored, maintained, and updated in a distributed manner in a peer-to-peer network. A blockchain can be associated with a cryptocurrency application, such as Bitcoin or Ethereum, Ripple, Dash, Litecoin, Dogecoin, zCash, Tether, Bitcoin Cash, Cardano, Stellar, EOS, NEO, NEM, Bitshares, Decred, Augur, Komodo, PIVX, Waves, Steem, Monero, Golem, Stratis, Bytecoin, Ardor, or digital currency exchanges, such as Coinbase, Kraken, CEX.IO, Shapeshift, Poloniex, Bitstamp, Coinmama, Bisq, LocalBitcoins, Gemini and others.

[0041] A "blockchain network" can include a computer network that maintains a blockchain. A blockchain network includes nodes that perform processing to maintain a blockchain.

[0042] A "block header" can be a header including information regarding a block in a blockchain. A block header can be used to identify a particular block on a blockchain. A block header can comprise any suitable information, such as a previous hash, a Merkle root, a timestamp, and a nonce. In some embodiments, a block header can also include a difficulty value.

[0043] A "cryptocurrency" can include a digital currency. A cryptocurrency can include a digital currency in which transactions are verified and records maintained by a decentralized system using cryptography. A cryptocurrency may not need to be maintained by a centralized authority.

[0044] A "cryptocurrency blockchain" can include a blockchain that stores cryptocurrency. A cryptocurrency blockchain can be utilized to transfer cryptocurrency from one public address to another public address.

[0045] An "interaction" may include a reciprocal action or influence. An interaction can include a communication, contact, or exchange between parties, devices, and/or entities. Example interactions include a transaction between two parties and a data exchange between two devices. In some embodiments, an interaction can include a user requesting access to secure data, a secure webpage, a secure location, and the like. In other embodiments, an interaction can include a payment transaction in which two devices can interact to facilitate a payment. An interaction can be a transfer of a resource from a first entity to a second entity.

[0046] A "resource" can include digital items and/or physical items. A resource can be an item that is obtainable. A resource can be owned by an entity. A resource can be a physical item such as goods, etc. A resource can be a digital item such as non-fungible tokens, etc.

[0047] A "processing network computer" may include a server computer used for interaction processing. In some embodiments, the network processing network 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 network processing network 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. In some embodiments, a network processing network computer may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. An exemplary network processing network computer may include VisaNet™. Networks that include VisaNet™ are able to process credit card transactions, debit card transactions, and other types of commercial transactions. VisaNet™, in particular, includes an integrated payments system (Integrated Payments system) which processes authorization requests and a Base II system, which performs clearing and settlement services. The network processing network computer may use any suitable wired or wireless network, including the Internet.

[0048] The processing network computer may process interaction-related messages (e.g., authorization request messages and authorization response messages) and determine the appropriate destination computer (e.g., an issuer computer) for the interaction-related messages. In some embodiments, the network processing network computer may authorize interactions on behalf of an issuer. The network processing network computer may also manage and/or facilitate the clearing and settlement of interactions. In some cases, the network processing network computer can include a token service computer, which can perform tokenization and/or de-tokenization services as described above.

[0049] An "authorization request message" may be an electronic message that requests authorization for an interaction. In some embodiments, it is sent to a transaction processing network computer and/or an issuer of a payment card to request authorization for a transaction. An authorization request message according to some embodiments may comply with International Organization for Standardization (ISO) 8583, which is a standard for systems that exchange electronic transaction information associated with a payment made by a user using a payment device or payment account. The authorization request message may include an issuer account identifier that may be associated with a payment device or payment account. An authorization request message may also comprise additional data elements corresponding to "identification information" including, by way of example only: a service code, a CVV (card verification value), a dCVV (dynamic card verification value), a PAN (primary account number or "account number"), a payment token, a username, an expiration date, etc. An authorization request message may also comprise "transaction information," such as any information associated with a current transaction, such as the transaction value, merchant identifier, merchant location, acquirer bank identification number (BIN), card acceptor ID, information identifying items being purchased, etc., as well as any other information that may be utilized in determining whether to identify and/or authorize a transaction.

[0050] An "authorization response message" may be a message that responds to an authorization request. In some cases, it may be an electronic message reply to an authorization request message generated by an issuing financial institution or a transaction processing network computer. The authorization response message may include, by way of example only, one or more of the following status indicators:

Approval -- transaction was approved; Decline -- transaction was not approved; or Call Center -- response pending more information, merchant must call the toll-free authorization phone number. The authorization response message may also include an authorization code, which may be a code that a credit card issuing bank returns in response to an authorization request message in an electronic message (either directly or through the transaction processing network computer) to the merchant's access device (e.g., POS equipment) that indicates approval of the transaction. The code may serve as proof of authorization.

[0051] 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 authorizing entity may operate an authorizing entity computer. An "issuer" may refer to a business entity (e.g., a bank) that issues and optionally 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, or in some embodiments, a portable device.

[0052] The term "verification" and its derivatives may include a process that utilizes information to determine whether an underlying subject is valid under a given set of circumstances. Verification may include any comparison of information to ensure some data or information is correct, valid, accurate, legitimate, and/or in good standing.

[0053] A "processor" may include a device that processes something. In some embodiments, a processor can include any suitable data computation device or devices. A processor may comprise one or more microprocessors working together to accomplish a desired function. The processor may include a CPU comprising at least one high-speed data processor adequate to execute program components for executing user and/or system-generated requests. The CPU may be a microprocessor such as AMD's Athlon, Duron and/or Opteron; IBM and/or Motorola's PowerPC; IBM's and Sony's Cell processor; Intel's Celeron, Itanium, Pentium, Xeon, and/or XScale; and/or the like processor(s).

[0054] A "memory" may be any suitable device or devices that can store electronic data. A suitable memory may comprise a non-transitory computer readable medium that stores instructions that can be executed by a processor to implement a

desired method. Examples of memories may comprise one or more memory chips, disk drives, etc. Such memories may operate using any suitable electrical, optical, and/or magnetic mode of operation.

[0055] 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 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.

DETAILED DESCRIPTION

[0056] As further described with reference to the figures below, authorization, clearing, and settlement can occur for a transaction initiated by a user that has a non-custodial cryptocurrency wallet on a wallet server and a payment device such as a payment card. The transaction can be initiated by the user. The user can interact the payment device with a resource provider computer (e.g., a merchant computer). The resource provider computer can transmit an authorization request message to a processing network computer in a payment processing network. The authorization request message can be transmitted from the processing network computer to an authorizing entity computer, which can have or communicate with a wallet server operated by a fintech. A transfer of the amount of cryptocurrency related or corresponding to the transaction can be transferred, by the wallet server, from the user's non-custodial cryptocurrency account to a third-party settlement account on the blockchain.

[0057] In embodiments, methods are provided, which enable access to funds from non-custodial wallets while integrating with existing payment transaction flows. An authorizing entity computer, using a fintech wallet server computer, can access the non-custodial wallet to validate presence of funds in the user's account and can settle transactions through the use of smart contracts. A processing network can allow funds from a non-custodial wallet to be transferred to a resource provider account managed by a transport computer such as an acquirer computer.

[0058] FIG. 1 shows a system according to an embodiment. The system 10 shows a user device 20 that can interact with a resource provider computer 50. The user device 20 can be in the form of a communication device 20A such as a laptop computer, or an access card 20B such as a payment card (e.g., a credit or debit card). The user devices 20A, 20B can store credentials or tokens, which are tied to a user blockchain address. The user devices 20A, 20B may or may not store a private key associated with the blockchain address. In some embodiments, the payment card may resemble a conventional chip or magstripe payment card.

[0059] The user device 20 can communicate with a resource provider computer 50, which may be in the form of an access device (e.g., a terminal such as a POS terminal or a remote e-commerce server). The resource provider computer 50 can be in communication with a transport computer 60 (e.g., an acquirer computer), a processing network computer 70 (e.g., a payment processing network computer), and an authorizing entity computer 80. The authorizing entity computer 80 can be in communication with a blockchain network 40. The blockchain network 40 can manage a blockchain for a digital currency such as a cryptocurrency.

[0060] In some embodiments, the authorizing entity computer 80 can manage and store an authorizing entity computer public key and an authorizing entity computer private key. The authorizing entity computer private key can be used to sign transactions on the blockchain. The authorizing entity computer 80 can also store private keys of user public-private key pairs for various users so that the authorizing entity computer 80 can conduct transactions on behalf of the users. The private keys may be stored in a secure memory such as a secure element or hardware security module. Also, in some embodiments, the authorizing entity computer 80 can comprise a first component that performs authorization and settlement processing for conventional payment device transactions, and a second component that performs cryptocurrency transactions for cryptocurrency accounts. In some embodiments, the first component could be an issuer computer and the second component could be a cryptocurrency digital wallet application server computer, which may communicate via an appropriate API (application programming interface). In other embodiments, the first and the second components may be first and second server computers, or first and second software modules in a single server computer.

[0061] In some embodiments, the user device 20, the resource provider computer 50, the transport computer 60, the processing network computer 70, and the authorizing entity computer 80 may be characterized as off-chain components, but may have the necessary cryptographic keys to allow them to interact with the blockchain in the blockchain network 40.

[0062] For simplicity of illustration, a certain number of components are shown in FIG. 1. It is understood, however, that embodiments of the invention may include more than one of each component. In addition, some embodiments of the invention may include fewer than or greater than all of the components shown in FIG. 1.

[0063] Messages between the devices included in the system 10 illustrated in FIG. 1 can be transmitted using a secure communications protocol 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 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.

[0064] Prior to conducting interactions with the system illustrated in FIG. 1, a user of the user device 20 can have an account such as a cryptocurrency account with the entity that is associated with the authorizing entity computer 80. The authorizing entity computer 80 can store the public and private key of the user on behalf of the user. The public key may be associated with a blockchain address associated with the user on the blockchain network 40. For example, the blockchain address of the user can be associated with, derived from, or be the public key of the user. Further, the user may register with the authorizing entity associated with the authorizing entity

computer to associate a credential and/or a token that is associated with the blockchain address. The authorizing entity computer 40 can obtain (e.g., generate or retrieve) the credential and/or token and then store it/them in a database in association with the blockchain address of the user. In some embodiments, the credential and/or the token does not have an underlying fiat currency account associated with it/them. The credential and/or the token can be stored in the user device 20, or can be retrievable by the user device 20 if the credential and/or the token is stored in the cloud.

[0065] FIG. 1 illustrates an example system 10 for authorizing a transaction conducted by a user using a non-custodial cryptocurrency wallet. FIG. 1 illustrates steps which allow for the authorization of a transaction which is based on the verification of cryptocurrency or other crypto assets in a non-custodial cardholder wallet.

[0066] At step S2, a user or can initiate an interaction with the resource provider computer 50 operated by a resource provider. In some embodiments, the interaction may be a payment transaction. The transaction may be to obtain a resource from the resource provider. The resource may be associated with a value, such as a fiat currency value or a cryptocurrency value. The resource provider can be a merchant and the resource provider computer can be a merchant computer. The credential or token is transferred from the user device 20 to the resource provider computer 50 using either a contact mechanism or a contactless mechanism (e.g., NFC or near field communications).

[0067] One or more cryptograms may also be provided to the resource provider computer 50. One type of cryptogram is a transaction cryptogram that is generated using data from the resource provider computer 50 (e.g., a terminal or computer ID, a transaction amount, an unpredictable number etc.) and data from the user device 20 (e.g., a credential such as a PAN or token). This data are then signed using a private key or symmetric on the user device 20. Later, the processing network computer 70 can verify the cryptogram using a corresponding cryptographic key to confirm that the authorization request message is legitimate and has not been tampered with. Another type of cryptogram is a token cryptogram if the token is provided to the resource

provider computer 50. The token cryptogram can encode data including a transaction channel type (e.g., a in person indicator, an e-commerce indicator), etc.

[0068] At step S4, the resource provider computer 50 can generate an authorization request message comprising the credential or token, the one or more cryptograms, and the value. The value may be an amount of fiat currency or may be an amount of cryptocurrency used to obtain the resource. If the amount is an amount of cryptocurrency, then the authorization request message may also comprise a currency code indicating the type of cryptocurrency that is being used in the transaction. The resource provider computer 50 can then transmit the authorization request message to the transport computer 60. In some embodiments, the authorization request message can be an ISO 8583 message.

[0069] At step S4, the resource provider computer 50 can transmit the authorization request message to the transport computer 60.

[0070] At step S6, the transport computer 60 can transmit the authorization request message to the processing network computer 70. In some embodiments, the processing network computer 70 can be a computer in a processing network (e.g., Visa™) such as a payment processing network.

[0071] At step S8, the processing network computer can process the authorization request message and route the authorization request to the authorizing entity computer 80. If the authorization request message comprises a token, then the processing network computer 70 can detokenize or have a token service computer detokenize the token (e.g., a payment token) to obtain the real credential (e.g., a PAN or primary account number). The processing network computer 70 can then replace the token with the credential in the authorization request message and can then transmit the authorization request message comprising the credential to the authorizing entity computer 80. Further, if the value in the authorization request message is a fiat currency value, then the processing network computer 70 can convert the fiat currency value to a cryptocurrency value using an appropriate conversion factor. The cryptocurrency value can then replace the fiat currency value. In other embodiments, this value conversion can be performed by the authorizing entity computer 80. In yet other embodiments, this value conversion can take place during settlement processing as in FIG. 3, which is described below.

[0072] In some embodiments, the authorization request message can be evaluated using fraud evaluation systems like those used in the payment card industry. The fraud evaluation systems can evaluate whether the resource providers transmitting the authorization request messages are potentially fraudulent or have security weakness, whether the credential or token is suspected of past fraud or raises security issues, whether cryptograms in the authorization request message are valid (e.g., thereby proving that the current transaction is authentic, that the token in the authorization request message is used in the correct transaction channel), etc. Cryptographic keys may be used to verify (e.g., decrypt) that the cryptograms and confirm that the transactions being conducted are being legitimately conducted. The fraud evaluation systems can enhance the overall security of the transaction giving the users of the inventive system confidence that the transactions being conducted are legitimate.

[0073] At step S12, the authorizing entity computer 80, after receiving the authorization request message from the processing network computer 70, can look up the blockchain address of the user (e.g., a cryptocurrency address of the user) associated with the credential. The blockchain address of the user can be an example of a first blockchain address. The authorizing entity computer 80 can initiate a blockchain transaction for the amount of the transaction or a derivative of the amount. In some embodiments, the blockchain account of the user can be based on stablecoins, such as US Dollar Coin (USD Coin) or Tether (₮ or USDT), which are designed to be equal to the U.S. dollar.

[0074] The authorizing entity computer 80 can submit a first blockchain transaction request comprising the amount or a derivative thereof (e.g., a conversion of the original amount, or an amount that is the original amount in the authorization request message less fees of some sort), the user's blockchain address (an example of a first blockchain address) to a blockchain address associated with the authorizing entity computer 80, and a digital signature to the blockchain network 40. The blockchain address associated with the authorizing entity computer 80 can be an example of a second blockchain address. The authorizing entity computer 80 can combine (e.g., concatenate) the data elements in the transaction request and sign them using the private key of the user. Once submitted, the blockchain network 40 can process the first blockchain transaction using a suitable processing method (e.g.,

proof-of-work processing, proof-of-stake processing, consensus, etc.) for inclusion in the blockchain. In some embodiments, the authorizing entity computer 80 can use a smart contract on the blockchain to initiate the blockchain transaction.

[0075] In some embodiments, the authorizing entity computer 80 maintains a balance of the user's blockchain account. In this case, the authorizing entity computer 80 can generate and transmit an authorization response message to the processing network computer 70 before the transaction is included on the blockchain managed by the blockchain network 40 includes the transaction in the blockchain.

[0076] At step S16, the authorizing entity computer 80 transmits an authorization response message to the processing network computer 70. If the authorization request message transmitted in steps S4 and S6 included a token, then the processing network computer 70 can re-tokenize the credential to the token. It can then include the token in the authorization response message. Regardless of whether tokenization occurred, the processing network computer 70 can then transmit the authorization response message to the resource provider computer 50 via the transport computer 60 in steps S18 and S20.

[0077] FIG. 2 shows a flow diagram illustrating a clearing process according to embodiments after the authorization process in FIG. 1 is performed.

[0078] At step S102, the transport computer 60 can communicate with different resource provider computers including the resource provider computer 50. The different resource provider computers can be operated by different resource providers, and each resource provider can have an account (to receive funds) with the entity (e.g., an acquirer) that operates the transport computer 60. The transport computer 60 can generate and send a first clearing record with authorized transactions for the transactions conducted by the resource provider computers to the processing network computer 70.

[0079] At step S104, the processing network computer 70 may send a second clearing record, based on the received first clearing record in step S102 to the authorizing entity computer 80. The first clearing record and the second clearing record may be present in post-authorization request messages such as clearing messages. At step S106, the authorizing entity computer 80 can confirm the data received in step S104 is accurate, and matches the transactions in the second clearing

record to the transactions that were authorized in the authorization process described above with respect to FIG. 1.

[0080] FIG. 3 shows a flow diagram illustrating a settlement process according to embodiments. The process in FIG. 3 can occur after the methods described with respect to FIGs. 1 and 2. The process in FIG. 3 can occur on a period basis (e.g., daily).

[0081] At step S204, the processing network computer 70 can calculate net settlement positions between the various authorizing entities operating the authorizing entity computers and the various operating the transport computers, to calculate net amounts owed to entities operating the transport computers. For example, if the authorizing entity operating the authorizing entity computer 80 is obligated to provide X funds to the entity that operates the transport computer 60, and the entity that operates the transport computer 60 is obligated to provide Y funds, wherein X is greater than Y, then the authorizing entity computer 80 would transfer funds in the amount of the net amount owed (e.g., X-Y) to the transport computer 60.

[0082] At step 206, the processing network computer 70 can send a settlement report to the authorizing entity computer 80. The settlement report can be in a post-authorization request message. The authorizing entity computer 80 can parse the report to determine the settlement amount owed (an example of a first settlement amount or a first post-authorization amount).

[0083] At step 208, the authorizing entity computer 80 can generate and transmit a second blockchain transaction comprising a first settlement amount owed to the blockchain network 40. The first settlement amount may be associated with the authorization request message described with respect to FIG. 1. The blockchain transaction request for the blockchain transaction can comprise the first settlement amount, the blockchain address of the authorizing entity computer (an example of a second blockchain address), and a blockchain address associated with the processing network computer 70 (an example of a third blockchain address), and a digital signature. The digital signature can include the above data elements combined (e.g., concatenated) and signed by a private key associated with the authorizing entity computer 80. The blockchain network 40 can process the second blockchain

transaction using the same or similar protocol as the first blockchain transaction described above.

[**0084**] At step S210, before or after the second blockchain transaction has been incorporated into the blockchain, the authorizing entity computer 80 can transmit to the processing network computer 70 a notification that that the second blockchain transaction has been submitted to the blockchain network 40 or has been completed by the blockchain network 40.

[0085] After the notification is received by the processing network computer 70 from the authorizing entity computer 80, the processing network computer 70 has the value of the second blockchain transaction added to its account on the blockchain. It can then provide the value owed to the entity operating the transport computer 60, or a second post-authorization amount such as a second settlement amount, as either fiat currency (which is a different type of value than the blockchain currency) or a blockchain currency (e.g., a cryptocurrency). The second settlement amount includes at least the amount associated with the authorization request message in FIG. 1.

[0086] For example, in step S212A, if the resource provider and/or the entity operating the transport computer 60 wanted to receive funds as a blockchain value, then the processing network computer 70 could submit a third blockchain transaction to the blockchain network 40. The third blockchain transaction request for the third blockchain transaction could include the value that the transport computer 60 is supposed to receive as part of the net settlement process, a blockchain address associated with the transport computer 60, a blockchain address associated with the processing network computer 70, and a digital signature. The digital signature for the third blockchain transaction can include above data elements combined (e.g., concatenated) and signed using a private key of the processing network computer 70. The blockchain network 40 can process the third blockchain transaction using the same or similar protocol as the first and second blockchain transactions described above.

[0087] If the resource provider operating the resource provider computer 50 was to receive the blockchain currency, then the transport computer 60 could initiate a fourth blockchain transaction with the blockchain network 40 to transfer value due to the resource provider operating the resource provider computer 50. The fourth

blockchain transaction request for the fourth blockchain transaction could include the value that the resource provider operating the resource provider computer 50 is supposed to receive, a blockchain address associated with the transport computer 60, and a digital signature. The digital signature for the fourth blockchain transaction can include above data elements combined (e.g., concatenated) and signed using a private key of the transport computer 60. The blockchain network 40 can process the fourth blockchain transaction using the same or similar protocol as the first, second, and third blockchain transactions described above.

[0088] In other embodiments, if the resource provider and/or the entity operating the transport computer 60 wanted to receive funds as fiat currency, then the processing network computer 70 could transmit the settlement amount owed to the transport computer 60 in a fiat currency transaction (e.g., a wire transfer or ACH or automated clearing house transfer). If this is the case, then the entity operating the processing network computer 70 can have a sufficient pool of fiat currency funds or the ability to access fiat currency funds (e.g., through a currency exchange) to provide the fiat funds for any settlements that require it.

[**0089**] If the currency conversion did not occur in the authorization process, then the currency conversion may be determined at this stage. For example, the processing network computer 70 may have received a settlement amount in the form of a cryptocurrency such as USDC from the authorizing entity computer 80. It can then convert the USDC into fiat currency such as US dollars before providing the fiat currency to the transport computer 60.

[**0090**] At step S214, the transport computer 60 can make funds available to a resource provider operating the resource provider computer. The funds received, for example, in step S212B can be provided to the account of the resource provider.

[0091] FIG. 4 illustrates a diagram of a communication device 400 according to an embodiment. communication device 400 may be an example of a user device, and can include device hardware 404 coupled to a system memory 402.

[0092] Device hardware 404 may include a processor 406, a short range antenna 414, a long range antenna 416, input elements 410, a user interface 408, and output elements 412 (which may be part of the user interface 408). 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 406 can be implemented as one or more integrated circuits (e.g., one or more single core or multicore microprocessors and/or microcontrollers), and is used to control the operation of communication device 400. The processor 406 can execute a variety of programs in response to program code or computer-readable code stored in the system memory 402, and can maintain multiple concurrently executing programs or processes.

[0093] The long range antenna 416 may include one or more RF transceivers and/or connectors that can be used by the communication device 400 to communicate with other devices and/or to connect with external networks. The long range antenna 416 may be configured to communicate with a remote base station and a remote cellular or data network, over the air. The short range antenna 414 may be configured to communicate with external entities through a short range communication medium. The short range antenna 414 may comprise a contactless interface that can interact with a contactless interface of another device (e.g., a portable device). Examples of a contactless interface may include one or more radio frequency (RF) transceivers that can send and receive communications using near-field communications (NFC), or other radio frequency or wireless communication protocols. The user interface 408 can include any combination of input and output elements to allow a user to interact with and invoke the functionalities of the communication device 400.

[0094] The system memory 402 can be implemented using any combination of any number of non-volatile memories (e.g., flash memory) and volatile memories (e.g., DRAM, SRAM), or any other non-transitory storage medium, or a combination thereof media. The system memory 402 may store computer code, executable by the processor 406, for performing any of the functions described herein.

[0095] The system memory 402 may also store an interaction application 402A, an authentication module 402B, cryptography module 402C, credentials/tokens 402D, and an operating system 402E. The interaction application 402A may include instructions or code executable by the processor 406 for initiating and conducting a blockchain transaction via an authorizing entity computer. The interaction application 402A can be a non-custodial wallet in some examples. The authentication module 402B may comprise code, executable by the processor 406, to authenticate a user.

This can be performed using user secrets (e.g., passwords) or user biometrics. The cryptography module 402C may comprise cryptographic processing logic such as encryption, decryption, and signing algorithms. It may also store public and private keys associated with the user of the communication device.

[0096] FIG. 5 shows a block diagram of a node computer 500. The node computer 500 may include a processor 502 and a computer readable medium 504, a data storage 506 which can store a blockchain 506A as well as a mempool of transactions, and a network interface 508 coupled to the processor 502.

[0097] The computer readable medium 504 may comprise a communication module 504A, a blockchain processing module 504B, and a smart contract interaction module 504C.

[0098] The communication module 504A can comprise code, executable by the processor 502 to cause the processor 502 to communicate with external entities.

[0099] The blockchain processing module 504B may comprise code that causes the processor 502 to interaction and process transactions for including on a blockchain as described above.

[0100] The smart contract interaction module 504C may comprise code that causes the processor 502 to perform smart contract interactions.

[0101] FIG. 6 shows a block diagram of an authorizing entity computer 600 according to an embodiment. The authorizing entity computer 600 comprises a processor 602 and a computer readable medium 604, a data storage 606, and a network interface 608 coupled to the processor 602. The data storage 606 may include secure component such as a secure element or hardware security module for storing the private keys associated with the users that conduct blockchain transactions using an interaction application associated with the authorizing entity computer 600.

[0102] The computer readable medium 604 may comprise a communication module 604A, which may have similar functions as communication module 604A above, a cryptography module 604B which may have similar functions as cryptography module 402C above, and an authorization processing module 604C. The authorization processing module 604C may comprise code, executable by the processor 602 to initiate (e.g., generate) authorization request messages, transmit authorization

request messages, receive authorization response messages, etc. The computer readable medium 604 may further comprising a store application management module 604D which may provide support for interaction applications (e.g., non-custodial digital wallet applications) on user devices. The computer readable medium 604 may also comprise a blockchain interaction module 604E which may cause the processor 602 to interact with the blockchain network and the blockchain as described above.

[0103] The computer readable medium 604 may comprise a code, executable by the processor 602, for performing operations comprising: receiving, from a processing network computer, an authorization request message comprising an amount and a credential associated with a user as part of a transaction between a resource provider and the user; determining a first blockchain address associated with the user using the credential; initiating a first blockchain transaction of the amount or a derivative thereof on a blockchain managed by a blockchain network from the first blockchain address associated with the user to a second blockchain address associated with the authorizing entity computer; receiving, from the processing network computer, a post-authorization request message associated with the authorization request message; and initiating a second blockchain transaction transferring a first post-authorization amount associated with the amount from the second blockchain address to a third blockchain address associated with the processing network computer, wherein the processing network computer provides a second post-authorization amount including the amount to a transport computer.

[0104] FIG. 7 shows a block diagram of a processing network computer 700 according to an embodiment. The processing network computer 700 may comprise a processor 702, which may be coupled to a computer readable medium 704, data storage 706, and a network interface 708. The data storage 706 may contain access data such as tokens and/or account data, as well as mappings between access data, credentials, and/or communication device identifiers such as phone numbers, IP addresses, device identifiers, etc. The data storage 706 may also store a public-private key pair of the processing network computer 700, so that it can interact with the blockchain network.

[0105] The computer readable medium 704 may comprise a number of software modules including an authorization processing module 704A, a cryptography module

704B, a communication module 704C, a clearing and settlement module 704D, a blockchain interaction module 704E, and a token processing module 704F.

[0106] The authorization processing module 704A may comprise code that can cause the processor 702 to evaluate authorization request messages for transactions and determine if the transactions should be authorized. The authorization processing module 704A may also include code for routing or modifying authorization request and response messages as they pass between various parties such as authorizing entity computers (e.g., issuer computers) and transport computers (e.g., acquirer computers).

[0107] The cryptography module 704B may include any suitable encryption / decryption algorithms to encrypt data in embodiments of the invention. Suitable data encryption / decryption algorithms may include DES, triple DES, AES, etc. It may also store encryption keys that can be used with such encryption / decryption algorithms. The cryptography module 704B may utilize symmetric or asymmetric encryption techniques to encrypt and/or verify data. Cryptographic keys that may be used by the cryptography module 704B may be securely stored in the data storage 706.

[0108] The communication module 704C may comprise code that causes the processor 702 to generate messages, forward messages, reformat messages, and/or otherwise communicate with other entities.

[0109] The computer readable medium 704 may also comprise receiving an authorization request message, the authorization request message comprising an amount and a credential or a token associated with a user as part of an interaction with a resource provider; transmitting, to an authorizing entity computer, the authorization request message comprising the credential, wherein the authorizing entity computer determines a first blockchain address associated with the user using the credential, and initiates a first blockchain transaction of the amount or a derivative thereof on a blockchain managed by a blockchain network from the first blockchain address associated with the user to a second blockchain address associated with the authorizing entity computer; transmitting to the authorizing entity computer a post-authorization request message associated with the authorization request message, wherein the authorizing entity computer initiates a second blockchain transaction transferring a first post-authorization amount associated with the amount from the

second blockchain address to a third blockchain address associated with the processing network computer; and providing a second post-authorization amount including the amount to a transport computer associated with the resource provider.

[0110] FIG. 8 shows a diagram of a blockchain according to embodiments of the present invention. FIG. 8 includes a blockchain 800 comprising a first block 810 and a second block 840. The blockchain 800 can include any suitable number of blocks (e.g., 10, 500, 2000, 500000, etc.).

[0111] 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. A block is created by a computationally intensive process called proof-of-work in which valid blocks need to demonstrate a sufficient “difficulty" (i.e., sufficient computation power to create on average). If there are more than one available chains of blocks, then network participants (i.e., nodes) can download all blocks in all chains and follow the chain which has the highest total difficulty. This mechanism guarantees that, eventually, the network will agree on a single and valid chain, see [Garay et al, The Bitcoin backbone protocol: Analysis and applications. In *Advances in Cryptology - EUROCRYPT 2015*, pages 281–310, 2015], [Bitcoin Website. bitcoin.org], and [Rafael Pass, Lior Seeman, and Abhi Shelat. Analysis of the blockchain protocol in asynchronous networks. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *Advances in Cryptology – EUROCRYPT 2017*, pages 643–673, Cham, 2017. Springer International Publishing.], which are all incorporated herein by reference for all purposes.

[0112] The blockchain 800 can create a history of data deposits, messages, or entries in a series of blocks where each block contains a mathematical summary, called a hash, of the previous block. This creates a chain where any changes made to a block will change that block's hash, which must be recomputed and stored in the next block. This changes the hash of the next block, which must also be recomputed and so on until the end of the chain.

[0113] Although the hash can be simple to compute, rules may be imposed, which require the value of the hash to be below a certain threshold value (i.e., a difficulty value). In addition, the hash is based on a type of mathematical function that is not reversible. One cannot predict what input can be used to produce the desired

output. A valid hash is found by repeatedly adjusting a changeable value in the block, and recalculating the hash until it meets the validity requirements. The freely changeable value can be a nonce. The unpredictable nature of the hash considerably increases the difficulty of finding a nonce that produces a valid hash of the block.

[0114] As an example, the first block 810 can include a block header 820 and block entries 830. The block header 820 of the first block 810 can comprise a previous hash 812, a timestamp 814, a Merkle root 816, and a nonce 818.

[0115] The previous hash 812 can be a hash of the previous block's header. The previous hash 812 can be the result of a non-reversible mathematical computation using data from the previous block as the input. According to some embodiments, the computation used can include a SHA256 hash function. One of ordinary skill in the art would recognize that any suitable hash function could be used without departing from the spirit and scope of the present invention. The hash function can be designed so that any change to the data in the previous block results in an unpredictable change in the hash of that block. The previous hash 812 can be a link between blocks, chaining them together to form the blockchain 800.

[0116] When calculating the previous hash 812 for the previous block, a node can determine if the previous hash 812 can meet certain criteria defined by a difficulty value. In some embodiments, the difficulty value may include a number that the calculated hash must be less than. However, because the output of the hashing function is unpredictable, the output cannot be determined what input will result in an output that is less than the difficulty value before the hash is calculated. The nonce 818 can be used to vary the data content of the block, allowing for a large number of different outputs to be produced by the hash function in pursuit of an output that meets the difficulty value. This makes can make it computationally expensive to produce a valid block with a nonce 818 that produces a hash value meeting the criteria of the difficulty value.

[0117] The hash algorithms used for the previous hash 812 can include MD5, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256, SHA-3 or any suitable hash function. There is also no requirement that a hash be computed only once. The results of a hash function may be reused as inputs into another or the same hash function again multiple times in order to produce a final result. One of

ordinary skill in the art would recognize that any hash function could be used to compute the required hashing without departing from the spirit and scope of the present invention.

[0118] The Merkle root 816 can be a root of a Merkle tree, which can include a tree in which every leaf node is labelled with the hash of a data block, for example an entry. Each leaf of the Merkle tree can represent one of the entries. Each entry can be hashed together with a sibling node (i.e., entry) in the Merkle tree. Successively hashing sibling nodes in the Merkle tree can result in the Merkle root 816.

[0119] The block entries 830 can include interaction data and/or smart contracts. The block entries 830 can include any suitable number of entries. Example entries can include the data described above, such as witnesses, signed witnesses, digital signatures, interaction messages, unconditional payment data, proof of inclusions, other data related to the processing of an offline interaction between two user devices, etc. In some embodiments, an entry may be a null value, for example, in the case of the Merkle tree being a sparse Merkle tree.

[0120] In some embodiments, the number of entries in the block entries 830 may be limited by the overall size of the block (e.g., the first block 810). For example, the blocks on the blockchain may be limited by a certain amount of data (e.g., 1/2 MB, 1 MB, 2 MB, 5 MB, 10 MB, etc.). In other embodiments, the number of entries in the block entries 830 may be a predetermined number of entries. For example, the nodes in the verification network can determine that 1, 10, 150, 500, 1000, etc. entries can be included in the block entries 830. The entries can be transactions, user operations, smart contracts, etc.

[0121] The timestamp 814 can include a time that the block was created within a certain range of error. According to some embodiments of the present invention, the full nodes of the verification network can check the timestamp 814 against their own known time and can reject any block that seems to have an erroneous timestamp 814.

[0122] The nonce 818 can be a value adjusted by a full node while performing a proof-of-work process, as described herein. A nonce can be input into a hash function along with block data to determine the output hash value. A correct nonce (also referred to as a golden nonce) yields an output hash value that satisfies a predetermined criteria, such as being less than a difficulty value.

[0123] The second block 840 can be similar to the first block 810. For example, the second block 840 can include a block header 850 and block entries 860. The block header 850 of the second block 840 can comprise a previous hash 852, a timestamp 854, a Merkle root 856, and a nonce 858. The block entries 860 can include image data, interaction data, smart contracts, etc., and can be similar to the block entries 830.

[0124] Embodiments of the invention have a number of technical advantages. For example, embodiments of the invention can process resource provider interactions faster than it would otherwise be possible with conventional blockchain transactions. Some embodiments above can use authorization request and response messages that are used in typical payment card transactions. Instead of minutes or hours, the authorization transactions according to embodiments can be conducted within seconds. Further, embodiments of the invention can modify blockchain transaction processes so that they are "pull" transactions where the transaction is requested by the recipient of funds. Unlike conventional blockchain transactions, fraud and security mechanisms such as velocity checks, cryptogram verifications, user authentications, account verifications, etc. can be performed using embodiments of the invention. Further, embodiments of the invention are also scalable and can result in widespread adoption. Still further, real time money movement across an ecosystem by utilizing the blockchain, such that at point of sale funds can move over the blockchain from issuer to a processing network, to acquirer, and to merchant in a shorter period of time than conventional settlement transactions, speeding up the settlement of funds when using a payment credential. This includes over weekends and holidays when a traditional banking system is not serviceable for funds movements.

[0125] 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.

[0126] 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.

[0127] 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.

[0128] 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.

[0129] As used herein, the use of "a," "an," or "the" is intended to mean "at least one," unless specifically indicated to the contrary.

WHAT IS CLAIMED IS:

1. A method comprising:

receiving, by a processing network computer, an authorization request message for a transaction, the authorization request message comprising an amount and a credential or a token associated with a user as part of an interaction with a resource provider;

transmitting, by the processing network computer to an authorizing entity computer, the authorization request message comprising the credential, wherein the authorizing entity computer determines a first blockchain address associated with the user using the credential, and initiates a first blockchain transaction of the amount or a derivative thereof on a blockchain managed by a blockchain network from the first blockchain address associated with the user to a second blockchain address associated with the authorizing entity computer;

transmitting, by the processing network computer, to the authorizing entity computer a post-authorization request message associated with the authorization request message, wherein the authorizing entity computer initiates a second blockchain transaction transferring a first post-authorization amount associated with the amount from the second blockchain address to a third blockchain address associated with the processing network computer; and

providing, by the processing network computer, a second post-authorization amount including the amount to a transport computer associated with the resource provider.

2. The method of claim 1, wherein providing the second post-authorization amount comprises providing a different type of value associated with the amount to the transport computer.

3. The method of claim 1, wherein providing the second post-authorization amount comprises transferring the second post-authorization amount to a fourth blockchain address associated with the transport computer.

4. The method of claim 1, wherein the user operates a user device with a storage application storing the credential or the token.

5. The method of claim 1, wherein the authorization request message is received from a resource provider computer operated by the resource provider.

6. The method of claim 1, further comprising:

responsive to transmitting the authorization request message to the authorizing entity computer, receiving, by the processing network computer, an authorization response message from the authorizing entity computer; and

transmitting, by the processing network computer, the authorization response message to the transport computer.

7. The method of claim 1, wherein the blockchain network processes blockchain transaction using a consensus algorithm.

8. The method of claim 1, further comprising:

receiving, by the processing network computer from the transport computer, a first clearing record including data associated with the authorization request message; and

transmitting, by the processing network computer to the authorizing entity computer, a second clearing record including data associated with the authorization request message.

9. The method of claim 1, wherein authorizing entity computer comprises an authorization processing module comprising code for processing authorization request and response messages, and a blockchain interaction module comprising code for interacting with the blockchain network.

10. The method of claim 1, wherein authorizing entity computer comprises a first computer comprising an authorization processing module comprising code for processing authorization request and response messages, and a second computer comprising a blockchain interaction module comprising code for interacting with the blockchain network, wherein the first computer and the second computer communicate via an API (application programming interface).

11. The method of claim 1, further comprising:

determining, by the processing network computer, net settlement positions with respect to a plurality of authorizing entity computers including the authorizing entity computer, and a plurality of transport computers including the transport computer, wherein the second post-authorization amount is a net settlement amount for the transport computer with respect to the plurality of authorizing entity computers.

12. A processing network computer comprising:

a processor; and

a non-transitory computer readable medium, the non-transitory computer readable medium comprising code, executable by the processor, to perform operations comprising:

receiving an authorization request message, the authorization request message comprising an amount and a credential or a token associated with a user as part of an interaction with a resource provider;

transmitting, to an authorizing entity computer, the authorization request message comprising the credential, wherein the authorizing entity computer determines a first blockchain address associated with the user using the credential, and initiates a first blockchain transaction of the amount or a derivative thereof on a blockchain managed by a blockchain network from the first blockchain address associated with the user to a second blockchain address associated with the authorizing entity computer;

transmitting to the authorizing entity computer a post-authorization request message associated with the authorization request message, wherein the authorizing entity computer initiates a second blockchain transaction transferring a first post-authorization amount associated with the amount from the second blockchain address to a third blockchain address associated with the processing network computer; and

providing a second post-authorization amount including the amount to a transport computer associated with the resource provider.

13. A method comprising:

receiving, by an authorizing entity computer from a processing network computer, an authorization request message comprising an amount and a credential associated with a user as part of a transaction between a resource provider and the user;

determining, by the authorizing entity computer, a first blockchain address associated with the user using the credential;

initiating, by the authorizing entity computer, a first blockchain transaction of the amount or a derivative thereof on a blockchain managed by a blockchain network from the first blockchain address associated with the user to a second blockchain address associated with the authorizing entity computer;

receiving, by the authorizing entity computer from the processing network computer, a post-authorization request message associated with the authorization request message; and

initiating, by the authorizing entity computer, a second blockchain transaction transferring a first post-authorization amount associated with the amount from the second blockchain address to a third blockchain address associated with the processing network computer, wherein the processing network computer provides a second post-authorization amount including the amount to a transport computer.

14. The method of claim 13, wherein the blockchain network processes blockchain transaction using a proof-of-work algorithm.

15. The method of claim 13, further comprising:

receiving, from the processing network computer by the authorizing entity computer, a second clearing record including data associated with the authorization request message.

16. The method of claim 13, wherein the credential comprises a sixteen digit number, and is not tied to a fiat account of the user.

17. The method of claim 13, wherein the authorization request message is an ISO 8583 message.

18. The method of claim 13, further comprising:

transmitting, by the authorizing entity computer to the processing network computer, an authorization response message in response to the authorization request message.

19. The method of claim 13, wherein the authorizing entity computer stores a user private key for the user on behalf of the of the user, and wherein the method further comprises:

signing the first blockchain transaction with the user private key to produce a first blockchain transaction digital signature; and

providing the first blockchain transaction and the first blockchain transaction digital signature to the blockchain network for incorporation into the blockchain.

20. The method of claim 13, wherein the authorizing entity computer stores an authorizing entity computer private key, and wherein the method further comprises:

signing the second blockchain transaction with the authorizing entity computer private key to produce a second blockchain transaction digital signature; and

providing the second blockchain transaction and the second blockchain transaction digital signature to the blockchain network for incorporation into the blockchain.

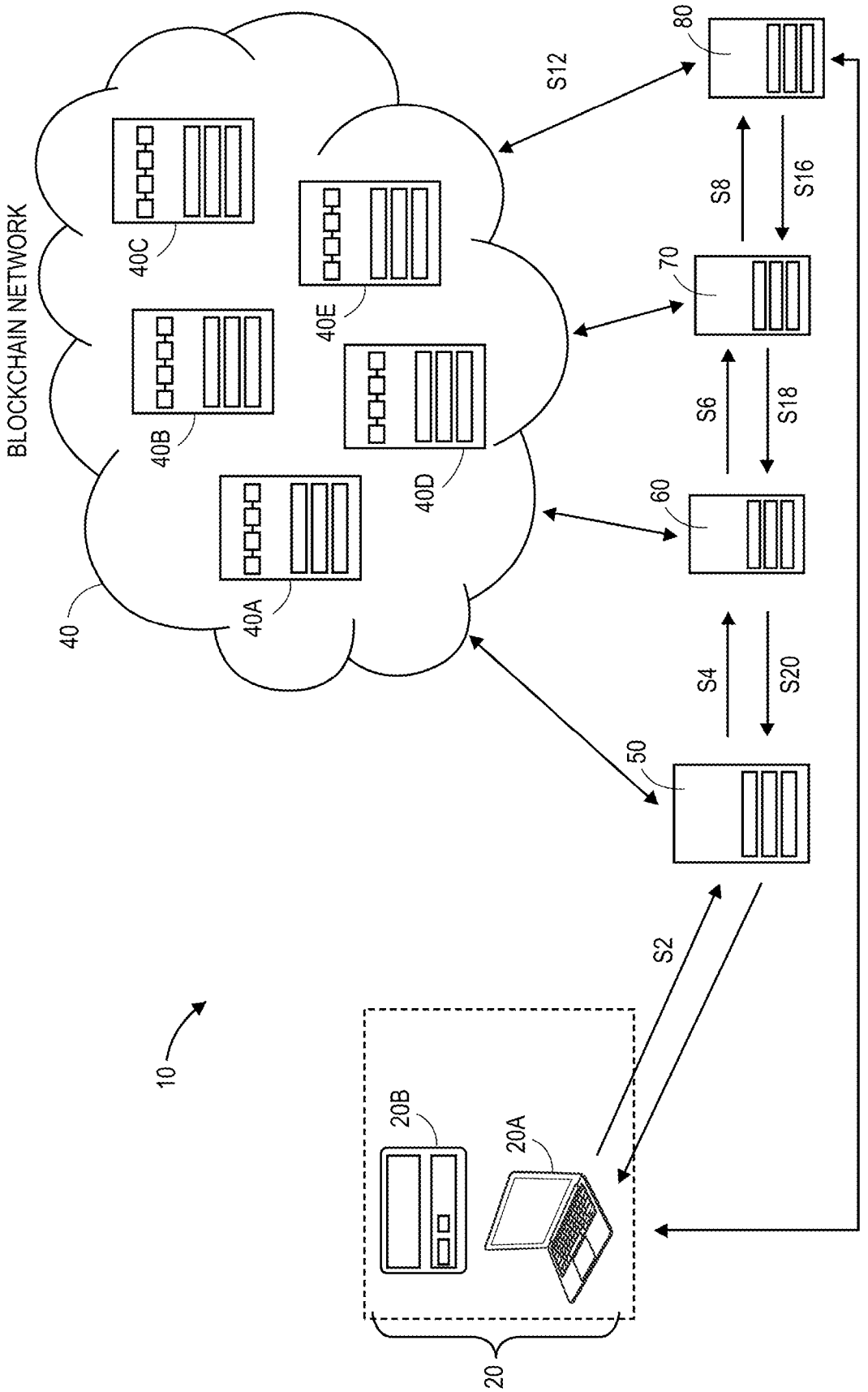
BLOCKCHAIN NETWORK
40
40A
40B
40C
40D
40E
S12
80
S8
S16
70
S6
S18
60
S4
S20
50
S2
10
20
20A
20B

FIG. 1

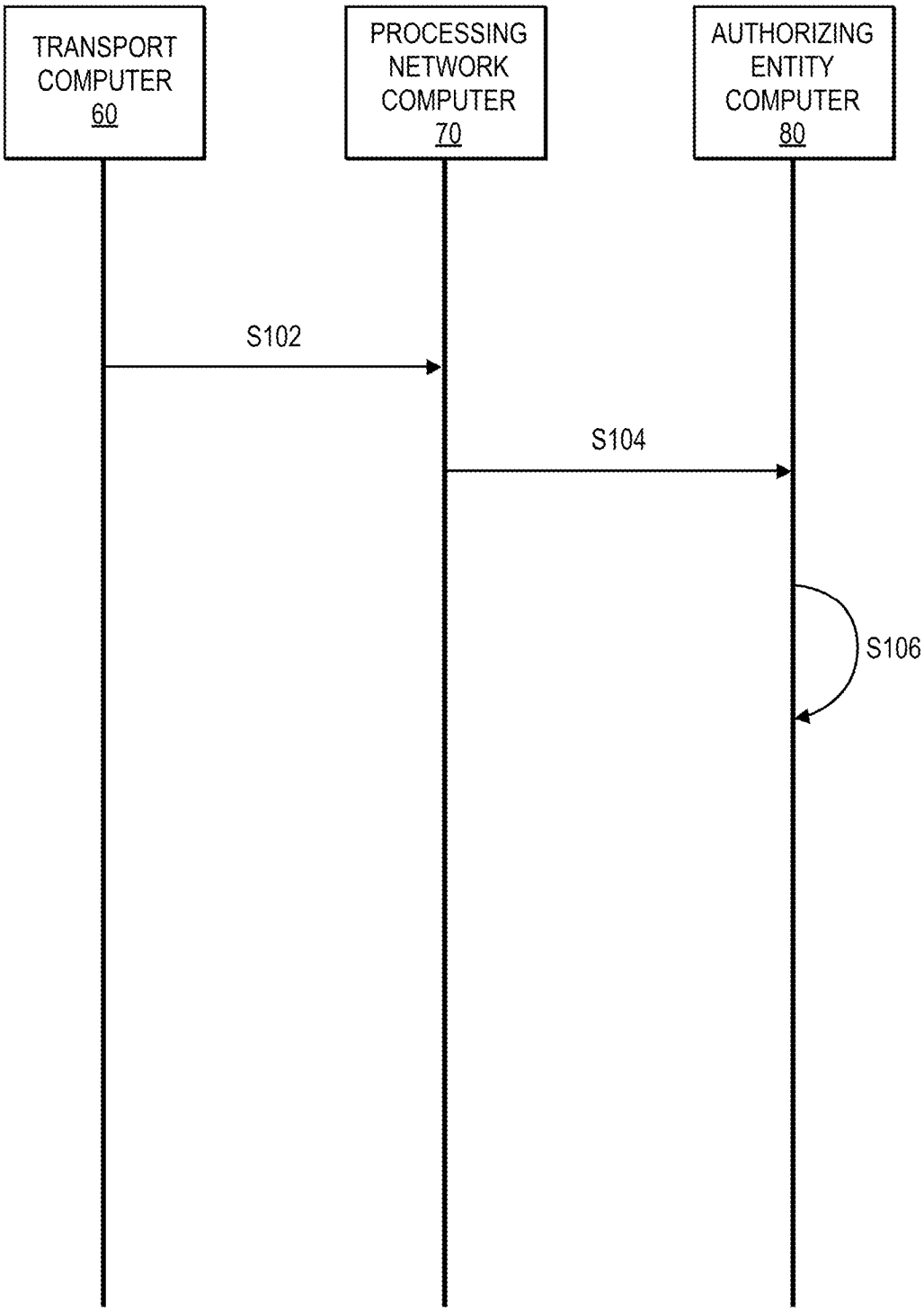
TRANSPORT COMPUTER 60
PROCESSING NETWORK COMPUTER 70
AUTHORIZING ENTITY COMPUTER 80
S102
S104
S106

FIG. 2

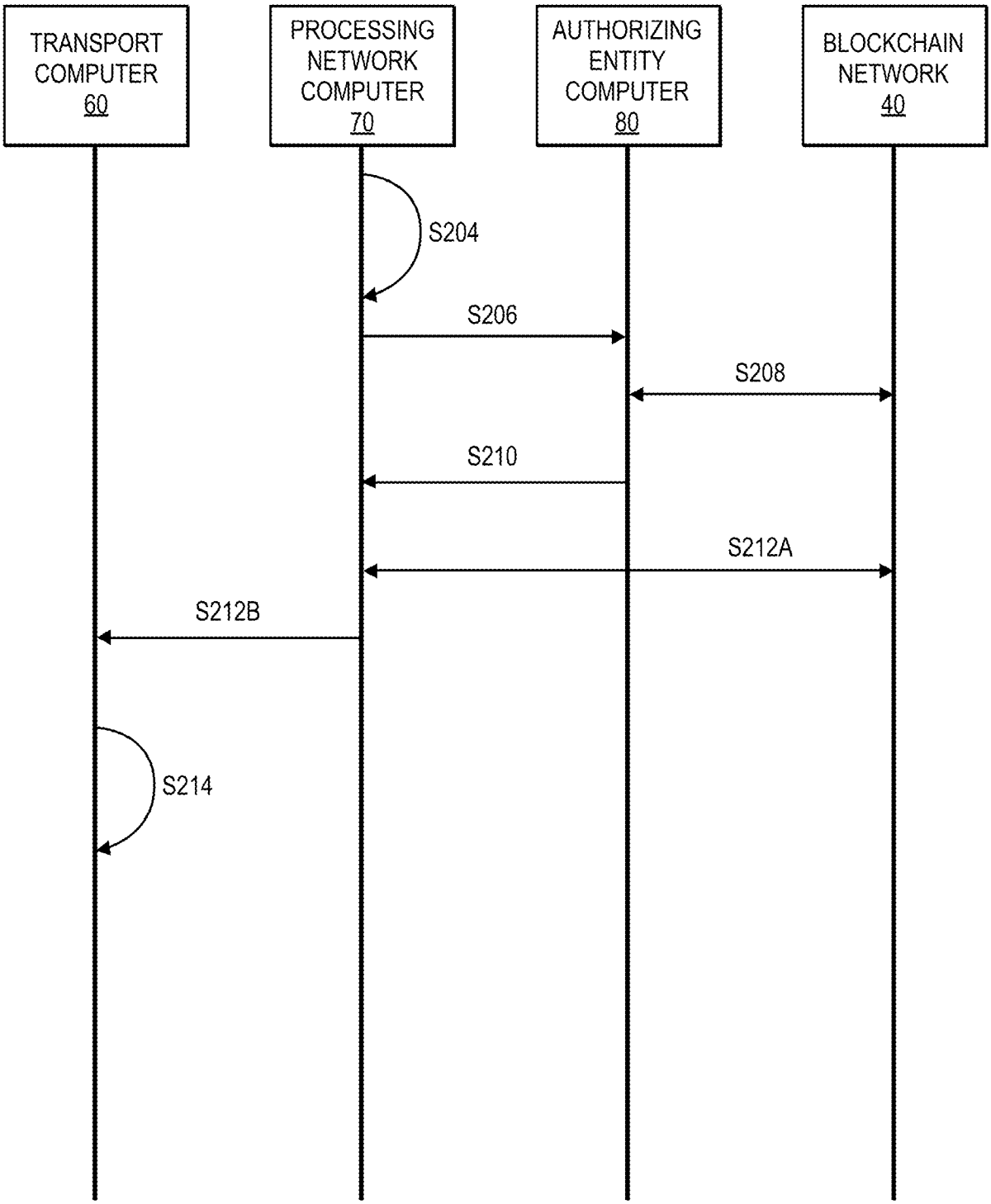
TRANSPORT COMPUTER 60
PROCESSING NETWORK COMPUTER 70
AUTHORIZING ENTITY COMPUTER 80
BLOCKCHAIN NETWORK 40
S204
S206
S208
S210
S212A
S212B
S214

FIG. 3

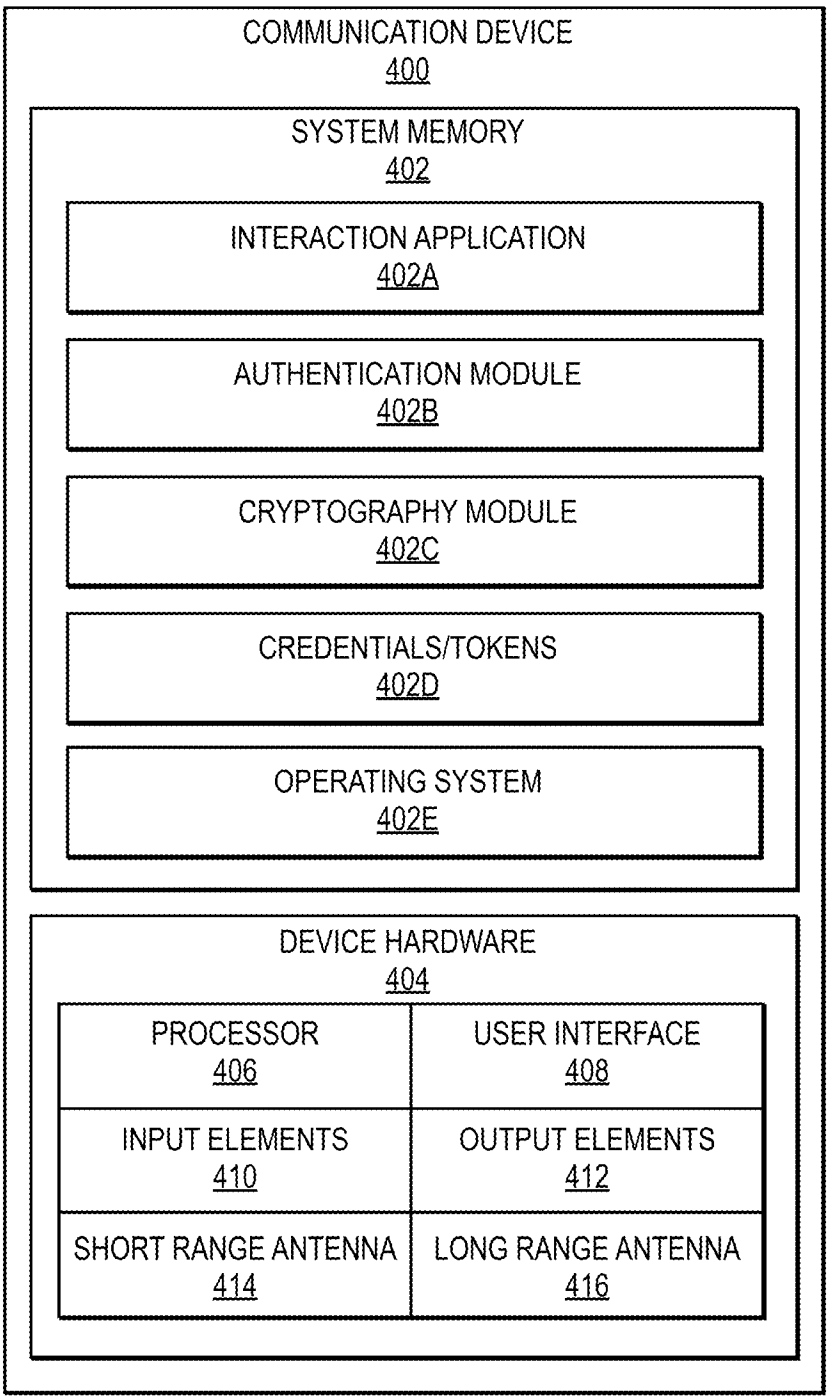
COMMUNICATION DEVICE
400
SYSTEM MEMORY
402
INTERACTION APPLICATION
402A
AUTHENTICATION MODULE
402B
CRYPTOGRAPHY MODULE
402C
CREDENTIALS/TOKENS
402D
OPERATING SYSTEM
402E
DEVICE HARDWARE
404
PROCESSOR
406
USER INTERFACE
408
INPUT ELEMENTS
410
OUTPUT ELEMENTS
412
SHORT RANGE ANTENNA
414
LONG RANGE ANTENNA
416

FIG. 4

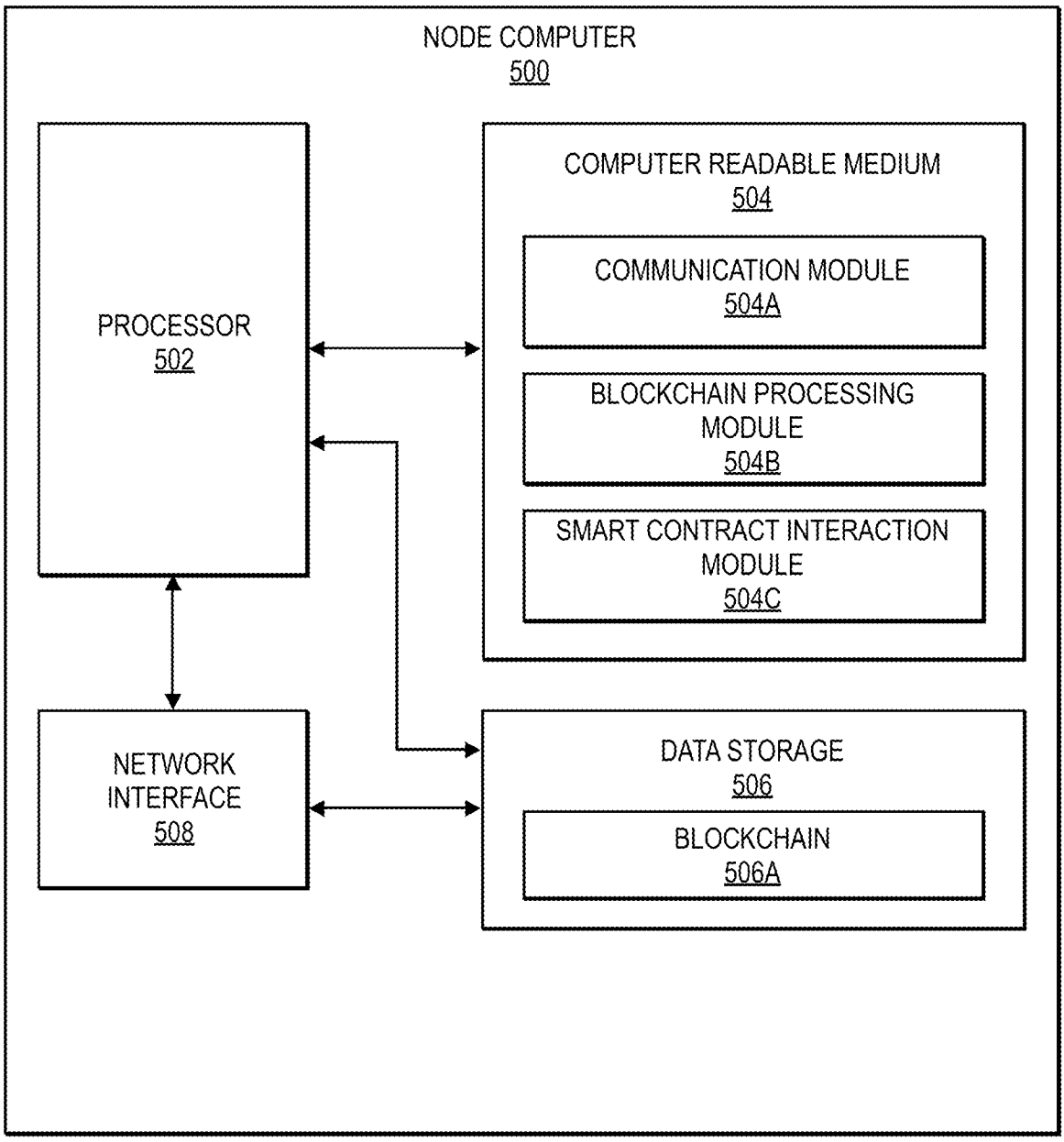
NODE COMPUTER
500
PROCESSOR
502
COMPUTER READABLE MEDIUM
504
COMMUNICATION MODULE
504A
BLOCKCHAIN PROCESSING MODULE
504B
SMART CONTRACT INTERACTION MODULE
504C
NETWORK INTERFACE
508
DATA STORAGE
506
BLOCKCHAIN
506A

FIG. 5

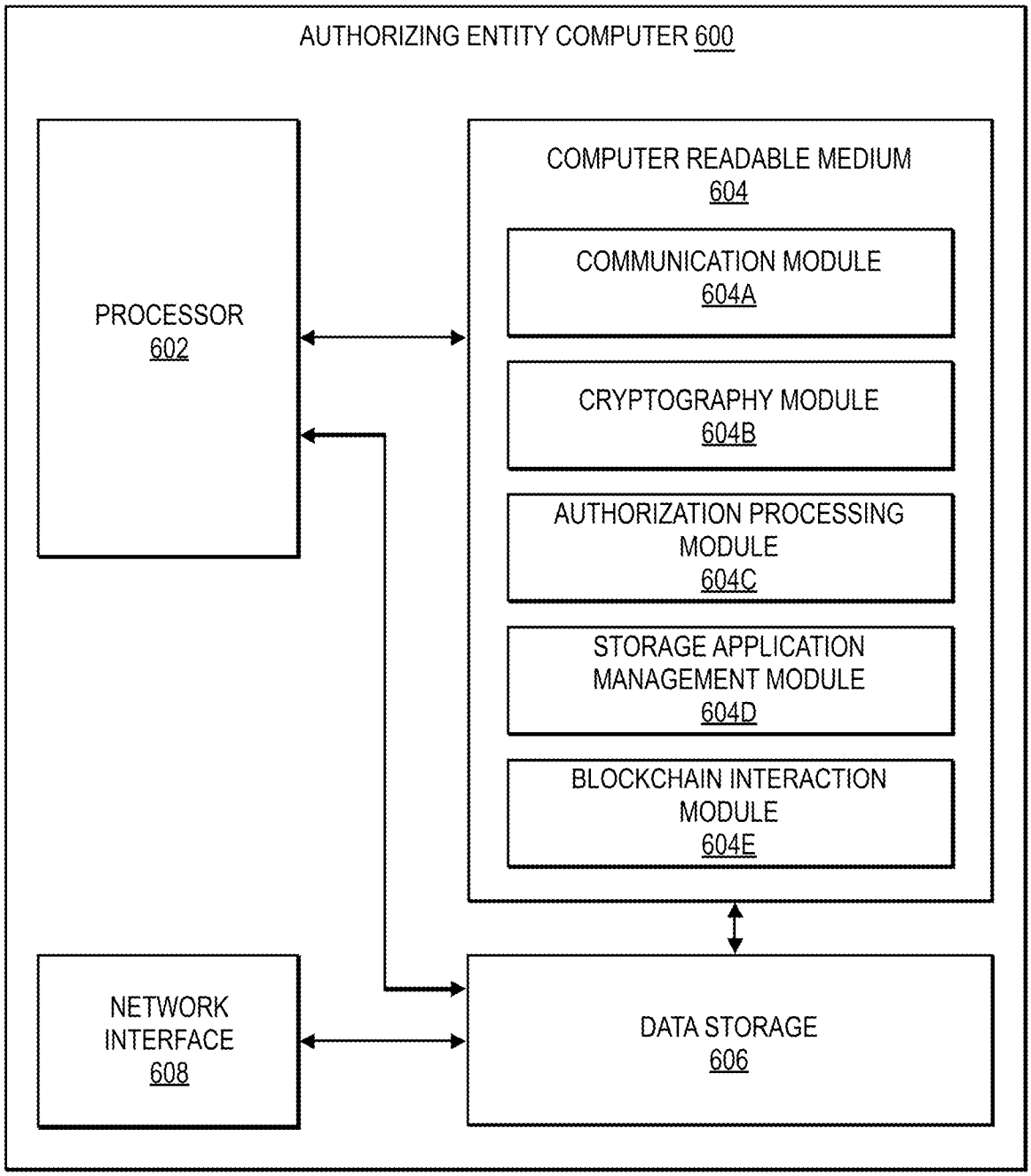
AUTHORIZING ENTITY COMPUTER 600
PROCESSOR 602
COMPUTER READABLE MEDIUM 604
COMMUNICATION MODULE 604A
CRYPTOGRAPHY MODULE 604B
AUTHORIZATION PROCESSING MODULE 604C
STORAGE APPLICATION MANAGEMENT MODULE 604D
BLOCKCHAIN INTERACTION MODULE 604E
NETWORK INTERFACE 608
DATA STORAGE 606

FIG. 6

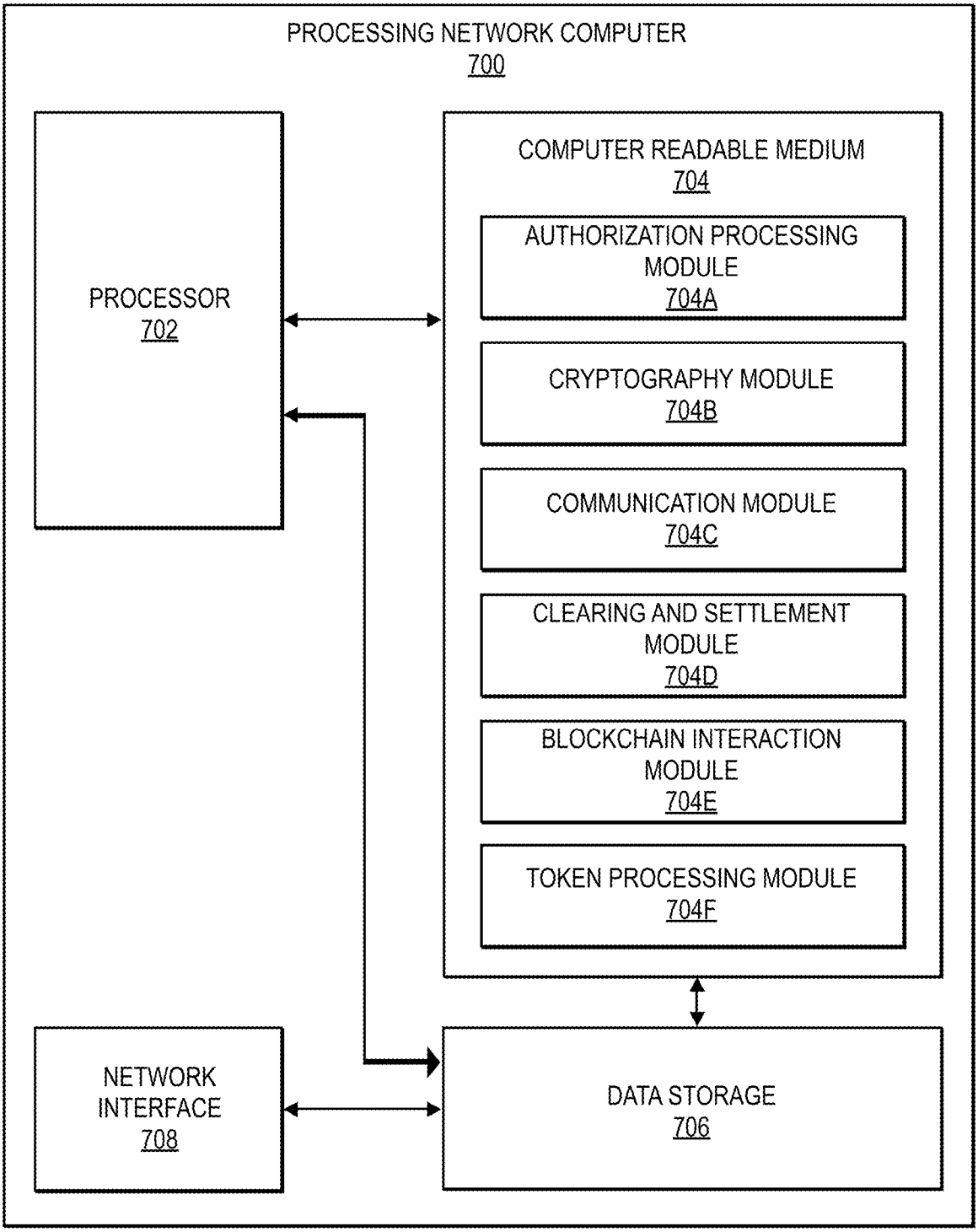
PROCESSING NETWORK COMPUTER
700
PROCESSOR
702
COMPUTER READABLE MEDIUM
704
AUTHORIZATION PROCESSING MODULE
704A
CRYPTOGRAPHY MODULE
704B
COMMUNICATION MODULE
704C
CLEARING AND SETTLEMENT MODULE
704D
BLOCKCHAIN INTERACTION MODULE
704E
TOKEN PROCESSING MODULE
704F
NETWORK INTERFACE
708
DATA STORAGE
706

FIG. 7

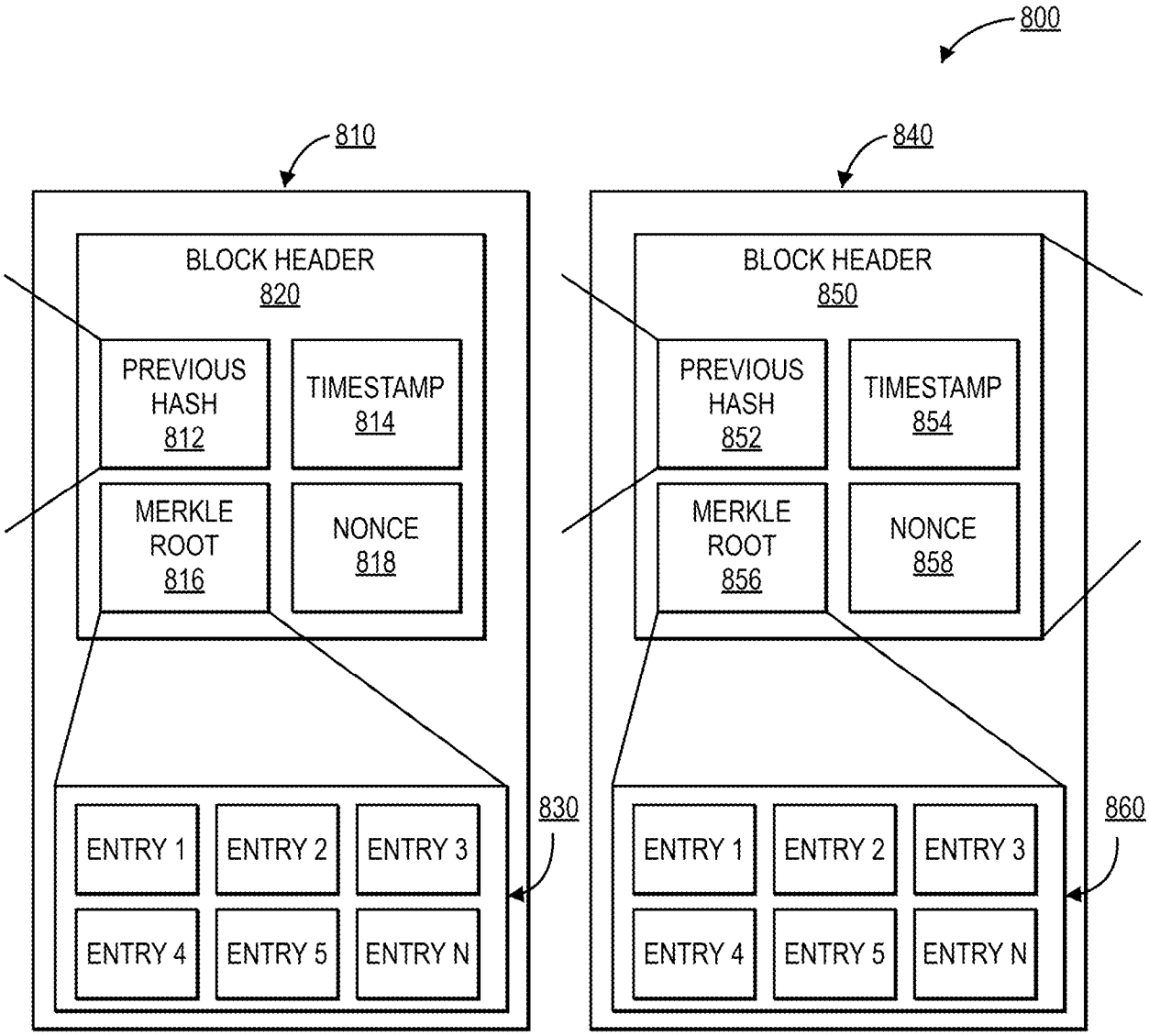
800
810
BLOCK HEADER
820
PREVIOUS HASH
812
TIMESTAMP
814
MERKLE ROOT
816
NONCE
818
830
ENTRY 1
ENTRY 2
ENTRY 3
ENTRY 4
ENTRY 5
ENTRY N
840
BLOCK HEADER
850
PREVIOUS HASH
852
TIMESTAMP
854
MERKLE ROOT
856
NONCE
858
860
ENTRY 1
ENTRY 2
ENTRY 3
ENTRY 4
ENTRY 5
ENTRY N

FIG. 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2024/035400

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/00(2006.01)i; **H04L 9/32**(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 9/00(2006.01); G06F 9/46(2006.01); G06Q 20/06(2012.01); G06Q 20/38(2012.01); G06Q 20/40(2012.01); H04L 9/32(2006.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & Keywords: blockchain, authorization request message, authorizing entity computer, credential, token

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2022-039726 A1 (VISA INTERNATIONAL SERVICE ASSOCIATION) 24 February 2022 (2022-02-24) paragraphs [0051]-[0101], claim 15 and figures 1-7	1-20
A	US 2023-0169495 A1 (MASTERCARD INTERNATIONAL INCORPORATED) 01 June 2023 (2023-06-01) paragraphs [0049]-[0060] and figures 3A-4	1-20
A	US 2022-0138745 A1 (TINGKAI LIU) 05 May 2022 (2022-05-05) paragraphs [0013]-[0102]	1-20
A	US 2023-0004423 A1 (REZA FATAHI et al.) 05 January 2023 (2023-01-05) paragraphs [0036]-[0056]	1-20
A	KR 10-2023-0014416 A (JEIWONCLOUD COMPANY) 30 January 2023 (2023-01-30) claims 1, 10, 11, 20	1-20

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"D" document cited by the applicant in the international application
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 September 2024	**02 October 2024**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office **189 Cheongsa-ro, Seo-gu, Daejeon** **35208, Republic of Korea**	**YANG, Jeong Rok**
Facsimile No. **+82-42-481-8578**	Telephone No. **+82-42-481-5709**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2024/035400

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
WO 2022-039726 A1	24 February 2022	CN 115956252 A	11 April 2023
		EP 4200781 A1	28 June 2023
		EP 4200781 A4	19 July 2023
		US 2023-0298009 A1	21 September 2023
US 2023-0169495 A1	01 June 2023	US 11556922 B2	17 January 2023
		US 2022-0374877 A1	24 November 2022
US 2022-0138745 A1	05 May 2022	US 11605080 B2	14 March 2023
US 2023-0004423 A1	05 January 2023	None	
KR 10-2023-0014416 A	30 January 2023	None	