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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 March 2020 (19.03.2020)

WIPO | PCT

(10) International Publication Number
WO 2020/055413 A1

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

(21) International Application Number:
PCT/US2018/050963

(22) International Filing Date:
13 September 2018 (13.09.2018)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **HITACHI, LTD.** [JP/JP]; 6-6, Marunouchi 1-chome, Chiyoda-Ku, Tokyo, 100-8280 (JP).

(72) Inventors; and
(71) Applicants: **SHIMAMURA, Atsushi** [JP/US]; c/o Hitachi America, Ltd., 3315 Scott Blvd., 4th Floor, Santa Clara, California 95054 (US). **PINSKI, David** [US/US]; c/o Hitachi America, Ltd., 3315 Scott Blvd., 4th Floor, Santa Clara, California 95054 (US).

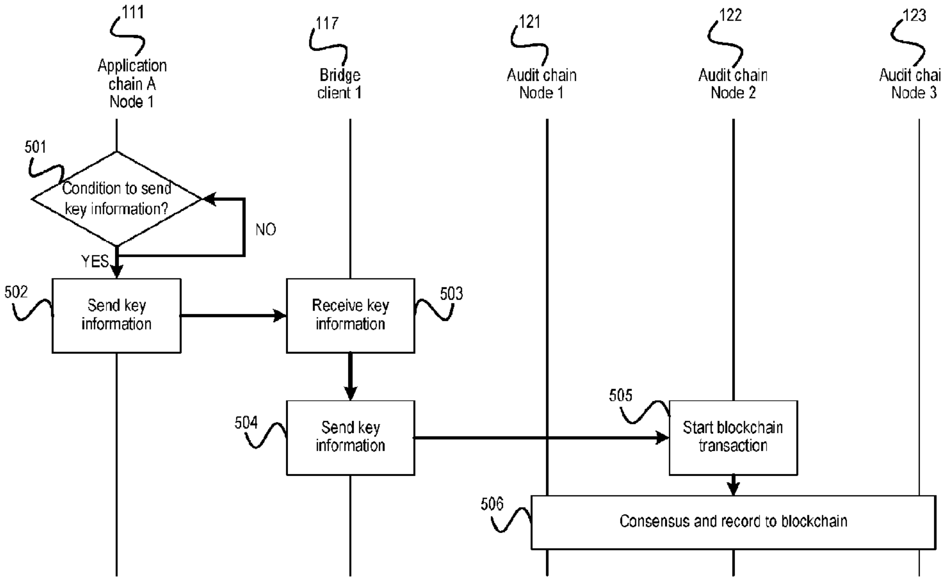
(74) Agent: **HUANG, Ernest C.** et al.; c/o Procopio, Cory, Hargreaves & Savitch LLP, 525 B Street, Suite 2200, San Diego, California 92101 (US).

(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, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, 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, 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).

(54) Title: BLOCKCHAIN FOR AUDIT

FIG. 5



(57) Abstract: In example implementations described herein, the audit chain is a blockchain network applied to ensure the immutability of multiple blockchain networks for various applications. Each blockchain for the application sends a hash value of block to audit chain. By storing the hash value in audit chain, each application blockchain can prove the status of the blockchain ledger in trustful manner.

[Continued on next page]

Published:

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

BLOCKCHAIN FOR AUDIT

BACKGROUND

Field

[0001] The present disclosure relates generally to blockchain related implementations, and more specifically, for auditing systems and methods for blockchain implementations.

Related Art

[0002] In the related art, there is a method for publishing hash values in log chain to various media, such as in a newspaper or in a web publication. However, such media cause problems with regards to cost, publishing frequency or immutability (e.g., little to no assurance for manipulation detection and protection). For example, newspapers are usually only published once or twice a day. So, the related art method can publish hash values a media such as a newspaper only once or twice in a day. Further, although publication on a webpage might allow a greater publication frequency, webpages are considered to be easily modifiable media.

[0003] In another related art implementation, there is a method for exchanging (crossing) hash values between log chains by using a crossing server. When two users conduct a transaction, they exchange their log chains through the crossing server, which causes such related art implementations to be limited to transactions between two parties. Thus, if N users conduct transactions between each other, they need a maximum of N x (N-1) /2 log crossing servers, and these N users need to have a relationship with all of the other members.

SUMMARY

[0004] The present disclosure is directed to system and methods for maintaining the integrity of a blockchain. In related art implementations, the hash values of the log chain are published on a newspaper or web publication server. However, example implementations described herein facilitate systems and methods to publish key information (such as hash value) of an application blockchain into another blockchain (such as an audit chain). In example implementations, an application blockchain involves a blockchain network, which has multiple nodes, and are used to conduct transactions or used to store transaction data.

[0005] Furthermore, example implementations described herein are directed to systems and methods for copying information from an audit chain into an application chain. Such data is recorded in an application blockchain to assure the status of the audit chain.

[0006] Aspects of the present disclosure includes a system, involving one or more first nodes configured to manage a plurality of first blockchains configured to manage transactions for a plurality of applications; and one or more second nodes configured to manage a second blockchain configured to manage integrity for the plurality of first blockchains; whereupon for an update to one of the plurality of first blockchains, the one or more first nodes are configured to generate key information associated with the one of the first blockchains and provide the key information to the one or more second nodes, wherein the one or more second nodes are configured to store the key information in the second blockchain.

[0007] Aspects of the present disclosure includes a system, involving means for managing a plurality of first blockchains configured to manage transactions for a plurality of applications; means for managing a second blockchain configured to manage integrity for the plurality of first blockchains; and whereupon for an update to one of the plurality of first blockchains, means for generating key information associated with the one of the first blockchains and means for storing the key information in the second blockchain.

[0008] Aspects of the present disclosure involve a non-transitory computer readable medium, storing instructions for executing a process, the instructions involving managing a plurality of first blockchains configured to manage transactions for a plurality of applications on one or more first nodes; managing a second blockchain configured to manage integrity for the plurality of first blockchains on one or more second nodes; and for an update to one of the plurality of first blockchains, generating key information associated with the one of the first blockchains and storing the key information in the second blockchain.

[0009] Aspects of the present disclosure involve a method, which involves managing a plurality of first blockchains configured to manage transactions for a plurality of applications on one or more first nodes; managing a second blockchain configured to manage integrity for the plurality of first blockchains on one or more second nodes; and for an update to one of the plurality of first blockchains, generating key information associated with the one of the first blockchains and storing the key information in the second blockchain.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] FIG. 1 illustrates an overall system upon which example implementations may be applied.

[0011] FIG. 2 illustrates an example hardware diagram for a node, in accordance with an example implementation.

[0012] FIG. 3 illustrates an example data structure stored in a blockchain, in accordance with an example implementation.

[0013] FIG. 4 illustrates an example of a chain between blocks, in accordance with an example implementation.

[0014] FIG. 5 illustrates an example flow diagram for copying key information, in accordance with an example implementation.

[0015] FIG. 6 illustrates the sample structure of key information, in accordance with an example implementation.

[0016] FIG. 7 illustrates an example of the block data in both application chain A and audit chain, in accordance with an example implementation.

[0017] FIG. 8 illustrates an example flow diagram of data propagation from audit chain, in accordance with an example implementation.

[0018] FIG. 9 illustrates an example structure of propagation data, in accordance with an example implementation.

[0019] FIG. 10 illustrates an example flow chart for finding a transaction among blockchain networks, in accordance with an example implementation.

[0020] FIG. 11 illustrates an example of index data that can be provided after a transaction to look up the transaction, in accordance with an example implementation.

DETAILED DESCRIPTION

[0021] The following detailed description provides further details of the figures and example implementations of the present application. Reference numerals and descriptions of redundant elements between figures are omitted for clarity. Terms used throughout the description are provided as examples and are not intended to be limiting. For example, the use of the term “automatic” may involve fully automatic or semi-automatic implementations involving user or administrator control over certain aspects of the implementation, depending on the desired implementation of one of ordinary skill in the art practicing implementations of the present application. Selection can be conducted by a user through a user interface or other input means, or can be implemented through a desired algorithm. Example implementations as described herein can be utilized either singularly or in combination and the functionality of the example implementations can be implemented through any means according to the desired implementations.

[0022] FIG. 1 illustrates an overall system upon which example implementations may be applied. Application chain A 110 illustrates an example blockchain network that can be applied for any application in accordance with the desired implementation. Application chain A can involve one or a plurality of nodes such as application chain A node 1 111, application chain A node 2 112, application chain A node 3 113, and the number of nodes can be adjusted to any number to facilitate the desired implementation. Further, there may be more application chains involved in the system, and they can also involve a similar structure as application chain A 110.

[0023] Application chain client 1 115 and Application chain client 2 116 are client systems of one node of application chain A 110. Such application chain clients are configured to send requests to application chain A 110, and receive data from application chain A 110. However, each node of the application chain A 110 can have any number of clients according to the desired implementation.

[0024] Audit chain 120 is an audit chain that is used to store some key information of application chain A 110. Audit chain 120 can involve one or a plurality of nodes, including audit chain node 1 121, audit chain node 2 112, audit chain node 3 113, and the number of nodes can be adjusted to any number to facilitate the desired implementation.

[0025] Audit chain client 119 is a client system for a node of audit chain 120. Audit chain client 119 can send requests to audit chain 120, as well as receive data from audit chain 120. Each node of audit chain 120 can have any number of clients according to the desired implementation.

[0026] Bridge client 1 117 and bridge client 2 118 are special client systems, that facilitate connections between application chain A 110 and audit chain 120. There can be any number of bridge clients, and they can be connected to any node in application chain A 110 and audit chain 120, in accordance with the desired implementation.

[0027] FIG. 2 illustrates an example hardware diagram for a node, in accordance with an example implementation. Any of the application chain nodes and audit chain nodes can be in the form of the hardware diagram as illustrated in FIG. 2. Node may involve memory 210, local storage 220, communication interface 251, processor 252 and Input/Output (I/O) device 253.

[0028] Processor 252 can be in the form of physical hardware processors such as Central Processing Units (CPUs) or in some combination of hardware and software processors, and can be configured to load the program from local storage 220 into memory 210 and executes the program. Communication interface 251 can be in the form of a network interface facilitating connections to a wide area network (WAN) or internet. I/O device 253 can involve any device configured to facilitate input or output into the node, such as a keyboard, a display, a mouse, and so on depending on the desired implementation.

[0029] Local storage 220 stores consensus program 221, blockchain storage 222 and operating system 243. Consensus program 221 is program for executing transactions on a blockchain. Based on the consensus program 221, the node exchanges messages with other nodes, and make a consensus on the transaction. Then, the node stores the transaction data into blockchain storage 222 as blockchain. Operating system 243 is a common program configured to facilitate the basic functionalities.

[0030] In related art implementations of the blockchain network, the blockchain provides immutable data storage. However, such blockchains are at risk of manipulation by a malicious system administrator managing the nodes of a blockchain internally, or if some number (e.g., 1/3) of the nodes are hacked and rendered to be malicious. In such scenarios, the blockchain may be maliciously modified without the user being aware that the blockchain is providing invalid data.

[0031] To address such problems and as will be described herein, example implementations will involve one or more first nodes configured to manage a plurality of first blockchains configured to manage transactions for a plurality of applications as illustrated in application chain A 110 of FIG. 1 with the underlying node structure of FIG. 2 and one or more second nodes configured to manage a second blockchain configured to manage integrity for the plurality of first blockchains as illustrated in in audit chain 120 with the underlying node structure of FIG. 2. Transactions can be in the form as illustrated in FIG. 3. For an update to one of the plurality of first blockchains, the one or more first nodes are configured to generate key information associated with the one of the first blockchains as described with respect to FIGS. 5 and 6, and provide the key information to the one or more second nodes, wherein the one or more second nodes are configured to store the key information in the second blockchain as described in FIGS. 5-7. Such an update can be conducted periodically, in response to a transaction or a set of transactions, or set according to the desired implementation.

[0032] In such an example implementation, the audit chain will behave as an independent blockchain network to provide integrity of the other blockchain networks managed by the audit chain. Such an audit chain has advantages over the related art by ensuring that the blockchain cannot be altered maliciously without inconsistencies in the data occurring within the audit chain. As described herein, the audit chain will manage key information to provide evidence of the integrity of the other application blockchains, while being configured to not storing confidential information of other blockchains within the audit chain. As the audit chains will be operated on separate nodes from the application blockchain, such nodes can be managed by a third party and act as a generic audit service for multiple application blockchain networks (e.g., banking chains, invoicing chains, etc.). Further, such implementations can be managed on a blockchain platform that is different from that of the managed application blockchain networks, depending on the desired implementation.

[0033] Further, the above example implementation conveys an advantage by providing the audit chain separately in its own nodes, in comparison to related art auditing processes executed on the blockchain network, which executed internally within the nodes of the application blockchain and cannot provide evidence of its integrity outside of the blockchain network.

[0034] Further, the above example implementation conveys an advantage of the related art implementations that utilize costly signature implementations to publish hash values to a website or newspaper, as the audit chain manages the record itself and can be configured to provide evidence of a transaction to a requesting client device.

[0035] Depending on the desired implementation, the key information can involve one or more of a blockchain ledger status of the one of the plurality of first blockchains, network data associated with the one of the plurality of first blockchains, and transaction meta data as illustrated in FIG. 6. Key information can also involve a hash value of a block of data in the one of the plurality of first block chains associated with a most recent one of the transactions, and a time stamp as illustrated in FIG. 6.

[0036] In example implementations, the one or more second nodes are configured to generate propagation data associated with the second blockchain, and transmit the propagation data to the one or more first nodes; wherein the one or more first nodes are configured to store the propagation data in all of the plurality of first block chains as illustrated in FIG. 8. In such an example implementation, the hash values are provided to one or more application blockchains, and the application blockchains can store such hash values, thereby rendering it difficult to manipulate data even if a malicious attacker has control of one of the application blockchains and can also hack the audit chain. Such propagation can happen periodically in accordance with the desired implementation.

[0037] In example implementations, the one or more second nodes are configured to, for receipt of a request comprising index data associated with one of the transactions stored in the plurality of first blockchains, process the request to locate the one of the transactions in the plurality of first blockchains; and provide a result of the processing to a client device associated with the request as illustrated in FIG. 10.

[0038] FIG. 3 illustrates an example data structure stored in a blockchain, in accordance with an example implementation. Each blockchain node stores multiple blocks of data 300. Each block of data 300 can involve multiple fields. In an example implementation, block number 301 indicates the sequential number of the particular block. Hash value 302 of previous block is a mathematically calculated value from a previous block. Number of transactions 303 is the number indicating how many transactions are set in transactions data 310. Timestamp 304 indicates the date and time that the block was created. Transaction(s) data 310 include data from one or more transactions. Each transaction can be associated with transaction meta data 320 and transaction details 330.

[0039] Transaction meta data 320 is data related to a particular transaction, and can include the transaction identifier (ID) 321, timestamp 322, requester ID 323, requester transaction ID 324 and digital signature 325. Such data in transaction meta data 320 are meta data (common attributes) of transaction details 330. Transaction ID 321 is the identifier of the transaction in application chain 110. It is assigned by application chain A 110 in a consensus process. Timestamp 322 is the date and time of the transaction that is recorded in application chain 110. Requester ID 323 is the identifier of the entity that requested the transaction. In the example of FIG. 3, requester ID 323 is ID of the client of application chain A 110. Requester transaction ID 324 is the identifier of the transaction which was assigned by the requester of transaction (ex. payer of payment transaction, or lender of lending agreement). Digital signature 325 is the digital signature signed by the requester of the transaction. Transaction details 330 include various data about the details associated with the transaction. For example, if the transaction is a payment, transaction details 330 may include payer identification, payee identification, amount and payment data, depending on the desired implementation.

[0040] FIG. 4 illustrates an example of a chain between blocks, in accordance with an example implementation. Specifically, FIG. 4 illustrates an example of a number of fields described in FIG. 3 as arranged in a chain. Hash value of previous block 402 is calculated by using hash function (e.g., such as SHA256, or others). For example, the hash value of previous block 402 in block 400-2 is calculated by whole block 400-1. Hash value of previous block 402 in block 400-3 is calculated by whole block 400-2. Thus, all blocks are connected in a chain by the hash value of previous block 402.

[0041] If such blocks with hash value of previous block 402 are stored on multiple nodes of the blockchain network, the implementation makes it very difficult to alter the transactions data 410 without causing a mismatch between the block data and the hash value of previous block 402 in the next block.

[0042] FIG. 5 illustrates an example flow diagram for copying key information 700, in accordance with an example implementation. Key information 700 is information which includes at least some portion of the status information of application chain A 110, and/or some portion of the transaction information recorded in application chain A 110. First, application chain A node 1 111 judges whether the condition to send key information is met at 501. The condition can be changed based on requirements. For example, when a new block is recorded on the application chain A 110, the condition can be determined to be met. Or, depending on the desired implementation, when some predefined number of blocks (e.g., ten blocks) are recorded then the condition is met. If condition is not met (No), application chain A node 1 111 keeps checking at 501, otherwise (Yes) the flow proceeds to 502.

[0043] At 502, application chain A node 1 111 send key information 700 to bridge client 1 117. The bridge client 1 117 receives the key information 700 at 503, and send the key information 700 to audit chain node 2 122 at 504. In this example, bridge client 1 117 is connected to audit chain node 2 122 as illustrated in FIG. 1.

[0044] At 505, audit chain node 2 122 starts a blockchain transaction, and nodes in audit chain 120 make a consensus on the transaction and record it in the respective blockchain at 506. Such implementations can be conducted according to any known implementation for conducting blockchain transactions on a blockchain network. For example, nodes in audit chain 120 can execute a smart contract, make consensus on the result of smart contract, and record the input (e.g., key information 700) and output (e.g, output of smart contract).

[0045] Through the implementation of FIG. 5, key information which is generated by application chain A 110 is stored in audit chain 120. Audit chain 120 is also a blockchain network, so key information stored on the audit chain 120 is very difficult to alter (fabricate), which thereby increases the integrity of application chain A 110. Since key information is also recorded in audit chain 120, modifying data in application chain A 110 will cause an inconsistency with key information stored on audit chain 120.

[0046] FIG. 6 illustrates the sample structure of key information 600, in accordance with an example implementation. Key information 600 is can involve several fields as illustrated in FIG. 6. Blockchain name 601 is identification of blockchain network. By using this blockchain name 601, each blockchain network (ex. "Application Chain A") is distinguished. Block number 602 is the identification of the block in the blockchain network that is identified by blockchain name 601. Hash value of previous block 603 is a hash value address of the previous block connected to the blockchain. Number of transactions 604 describes the number of transactions in transactions data 310 of blockchain data 300 identified by block both blockchain name 601 and block number 602. Timestamp 605 is the date and time information indicating when key information 600 was created.

[0047] Transactions data 606 is similarly implemented as transactions data 310 from FIG. 3. Depending on the desired implementation, transactions data 606 may not have all of the transaction details 330. Some of data in transaction details 330 may be confidential or contain private information, so key information 600, which is sent from application chain 110 to its outside (audit chain 120) can omit such data and not include all of transaction details 330 depending on the desired implementation. For example, instead of transaction details 330, key information 600 may have transaction meta data 610 or transaction index data 616 or transaction hash value 617. Transaction meta data 610 is same data as transaction meta data 320 in block data 300. Transaction index data 616 is information representative of transaction details 330. The contents of the transaction index data 616 should be defined based on application run on application chain A 110. Transaction hash value 617 is hash value of transaction details 330. By including transaction hash value 617, the existence of transaction details 330 can be checked without contents of transaction details 330. Hash value of current block 620 is the hash value block which contains the corresponding block data 300. The value is also recorded to hash value of previous block 302 in the subsequent block in the blockchain.

[0048] Further, the data to be included in key information 600 is not limited to these data fields, and can be modified according to the desired implementation. Key information can include any information which application chain A 110 manages. For example, key information 600 can include the configuration information of the application chain A 110. Such information can involve information regarding the nodes (e.g., IP address, domain name, owner organization name), definition of blockchain network behavior (e.g., security group or boundary of data sharing), and so on depending on the desired implementation. Key information can also include smart contract information (e.g., name of smart contract), hash value of the smart contract program, parameters of the smart contract execution, smart contract installation information (e.g., date and time of installation, identification of user who installed it), and/or hash value of the data stored on the blockchain. For example, in some blockchain implementations, blockchain is used as a log for a database. In such a case, the database stores the current snapshot of data (e.g., if the blockchain is used for account management, the current balance of the account is snapshot without the past balances or transactions)).

[0049] FIG. 7 illustrates an example of the block data 300 in both application chain A 110 and audit chain 120, in accordance with an example implementation.

[0050] Block data 701 is one of the blocks of data 300 stored in audit chain node 1 121 (or other node in audit chain 120). Block data 702 is another one of the blocks of data 300 stored in application chain A node 1 111 (or other node in application chain A 110).

[0051] When block data 702 is stored in application chain A node 1 111, and application chain A node 1 judges that the condition to send key information is met (see step 501), application chain A node 1 send key information 600 (step 502). For example, application chain A node 1 111 send key information 600 which includes hash value of current block 620. This key information is sent to one node of audit chain 120, and the key information is stored in a part of transaction data 310 of blockchain data 300 in audit chain 120.

[0052] As illustrated in FIG. 7, hash value of blockchain block 702 is stored in transaction details 330 as key information 711. Thus, hash value of block data 300 in application chain A 110 is stored in audit chain 120. In such situations, the status of the application chain A 110 can be checked by the data in audit chain 120. To manipulate the data in application chain A 110, manipulation of audit chain 120 would also be required and is not feasible, which thereby prevents the manipulation of application chain A 110.

[0053] FIG. 8 illustrates an example flow diagram of data propagation from audit chain 120, in accordance with an example implementation. As shown in FIG. 5, application chains (for example, application chain A 110, although there can be multiple application chains depending on the desired implementation) can send key information 600 and audit chain 120 collects key information from multiple application chains.

[0054] In FIG. 8, data is sent from audit chain 120 to application chains (such as application chain 110) instead. As there are multiple application chains, if each application chain stores some status data of audit chain 120, it will be very difficult to manipulate the data in audit chain 120.

[0055] FIG. 8 is similar to FIG. 5, except for the data (in FIG. 8, propagation data) is sent from audit chain node 2 122 to application chain A node 1 111 via bridge client 1 117.

[0056] First, application audit chain node 2 122 judges whether the condition to send propagation data is met at 801. The condition can be changed based on requirements set according to the desired implementation. For example, when some predefined number of blocks (e.g., 100 blocks) are recorded then the condition is met in one example implementation. Or, if a certain time period has elapsed or the current time has passed a predefined time in the day (e.g., midnight), the condition is met in another example implementation. In FIG. 8, data can be sent to multiple application chains; depending on the desired implementation, the condition to send data is set to reduce the number of data than the number of data sent by the condition in FIG. 5.

[0057] Next, audit chain node 2 112 send propagation data 900 to bridge client 1 117 at 802.

[0058] The bridge client 1 117 receives the propagation data 900 at 803, and sends the propagation data 900 to application chain A node 1 111 at 804. Application chain A node 1 111 starts blockchain transaction at 805, and nodes in application chain A 110 make a consensus on the transaction and records it as blockchain at 806. Such implementations can be conducted according to any desired implementation of blockchain network and transactions. For example, nodes in application chain A 110 can execute a smart contract, make a consensus on the result of the smart contract, and record the input (e.g., propagation data 900) and output (output of smart contract). By the flow of FIG. 8, propagation data 900 which is generated by audit chain 120 is stored in audit chain 120. Application chain A 110 is also a blockchain network, so propagation data 900 stored on the application chain A 110 is very difficult to alter or fabricate.

[0059] Further, nodes in audit chain 120 can be connected to multiple application chains. In this example implementation, multiple nodes in audit chain 110 execute the same process as audit chain node 2 122 (step 801 and step 802) shown in FIG. 8. Then these multiple nodes send propagation data to multiple bridge clients, and multiple nodes in multiple application chains.

[0060] Thus, propagation data can be propagated to multiple application chains. Such implementations increases the integrity of audit chain 120. Further, because propagation data 900 is also recorded in multiple application chains, modifying data in audit chain 120 case will cause an inconsistency with propagation data stored on multiple application chains, which can be detected.

[0061] FIG. 9 illustrates an example structure of propagation data 900, in accordance with an example implementation. Propagation data 900 can include a blockchain name 901, block number 902, hash value 903 and timestamp 904. Blockchain name 901 is data to identify the blockchain network (e.g., “Audit Chain” or other name according to the desired implementation). If there are multiple audit chains 120 in the market, the blockchain name 901 is used to distinguish the source of the propagation data 900. Block number 902 identifies the block when the flow at 801 in FIG. 8 is executed. Hash value 903 is hash value calculated using block data 300 identified by block number 902. In the flow of 802 of FIG. 8, audit chain node 2 122 specifies the latest blockchain block 300 in the audit chain 120. Further, audit chain node 2 122 creates the propagation data 900 by setting the blockchain name 901 (this is previously stored on audit chain node 2 122) and block number 902 (this is copied from block number 301 of latest block chain block 300), and calculates the hash value 903 by using the whole block of data of the latest block chain block 300. Audit chain node 2 122 sets the current time into time stamp 904. By using hash value 903 of block data 300 in audit chain 120, propagation data 900 stored on multiple application chains assures the status of audit chain 120 at the timing of propagation.

[0062] FIG. 10 illustrates an example flow chart for finding a transaction among blockchain networks, in accordance with an example implementation. To facilitate verification of a transaction, the user of a blockchain network uses a blockchain via a client and can find the transaction on the blockchain. However, there may also be users that utilize the blockchain network indirectly (e.g., the trading partner of a user has access to a client of the blockchain). In this case, although the transaction might be executed on the blockchain network, the user might not have a direct relationship to the blockchain network or its client, even though the user is involved in the transaction on the blockchain. Thus, there is a need to facilitate implementations for identifying and checking the existence and contents of transaction recorded on blockchain. FIG. 10 illustrates an example implementation.

[0063] At first, when some transaction is done on application chain A 110, application chain A node 3 113 issues a transaction code and sends it to application chain client 2 116 at 1010. However, the present disclosure is not limited to application chain A 110 and application chain A node 3 113. Any blockchain network and any node can execute the flow diagram of FIG. 10 in accordance with the desired implementation.

[0064] At 1011, application chain client 2 116 create a user accessible transaction code 1100. Application chain client 2 116 sends or shows user accessible code 1100 to the user (e.g., examples of users can be an individual or organization who is involved or who is related to the transaction on blockchain). The user accessible code 1100 contains the information to identify the blockchain and the transaction (for example, blockchain name, block number, transaction number or hash value of transaction data).

[0065] When the user may need to view or check the transaction, or the user may need to share the existence or contents of a transaction to another, the user (or another, who needs to view or check the transaction) uses the user accessible code 1100 (user accessible code 1100 can be copied or can be sent to another).

[0066] When the user (or someone who received user accessible code 1100) needs to view or check the transaction, the user inputs the information of user accessible code 1100 to audit chain client 119. If user accessible code 1100 is text data, user inputs the code by keyboard through the audit chain client 110. If user accessible code 1100 is some visual code such as a quick release (QR) code illustrated in FIG. 11, audit chain client 119 captures the picture of user accessible code 1100 and decodes the visual code. User can use their own device or other terminal to input the information of user accessible code 1100 or scan the code, and the device or terminal sends the information to audit chain client 119.

[0067] At 1021, audit chain client 119 sends the code to one of the nodes of audit chain 120 (for example, audit chain node 3). At 1022, audit chain node 3 123 receives the request. At 1023, audit chain node 3 123, which is one of the nodes of audit chain 120, finds the targeted data from the blockchain stored on blockchain storage 222.

[0068] To find the transaction, audit chain node 3 123 use the information of user accessible code 1100 (Audit chain node 3 123 searches the blockchain storage 222 and find the key information data 600, which matches to the information of user accessible code 1100. For example, by comparing blockchain name 601, block number 602 transaction ID 611 and transaction index data 616, and transaction hash value 617, audit chain node 3 123 searches for the corresponding data.

[0069] Then, audit chain node 3 123 sends the result at 1024, and audit chain client 119 receives the results at 1025. Audit chain client 119 then provides the result to user (e.g., audit chain client 119 sends the result to the user device).

[0070] In an example implementation, the result can include all or some of transaction meta data 610 and transaction index data 616, depending on the desired implementation. If no key information 600 is found in the flow at 1023, then the result can indicate that no data was found.

[0071] Some portions of the detailed description are presented in terms of algorithms and symbolic representations of operations within a computer. These algorithmic descriptions and symbolic representations are the means used by those skilled in the data processing arts to convey the essence of their innovations to others skilled in the art. An algorithm is a series of defined steps leading to a desired end state or result. In example implementations, the steps carried out require physical manipulations of tangible quantities for achieving a tangible result.

[0072] Unless specifically stated otherwise, as apparent from the discussion, it is appreciated that throughout the description, discussions utilizing terms such as “processing,” “computing,” “calculating,” “determining,” “displaying,” or the like, can include the actions and processes of a computer system or other information processing device that manipulates and transforms data represented as physical (electronic) quantities within the computer system’s registers and memories into other data similarly represented as physical quantities within the computer system’s memories or registers or other information storage, transmission or display devices.

[0073] Example implementations may also relate to an apparatus for performing the operations herein. This apparatus may be specially constructed for the required purposes, or it may include one or more general-purpose computers selectively activated or reconfigured by one or more computer programs. Such computer programs may be stored in a computer readable medium, such as a computer-readable storage medium or a computer-readable signal medium. A computer-readable storage medium may involve tangible mediums such as, but not limited to optical disks, magnetic disks, read-only memories, random access memories, solid state devices and drives, or any other types of tangible or non-transitory media suitable for storing electronic information. A computer readable signal medium may include mediums such as carrier waves. The algorithms and displays presented herein are not inherently related to any particular computer or other apparatus. Computer programs can involve pure software implementations that involve instructions that perform the operations of the desired implementation.

[0074] Various general-purpose systems may be used with programs and modules in accordance with the examples herein, or it may prove convenient to construct a more specialized apparatus to perform desired method steps. In addition, the example implementations are not described with reference to any particular programming language. It will be appreciated that a variety of programming languages may be used to implement the teachings of the example implementations as described herein. The instructions of the programming language(s) may be executed by one or more processing devices, e.g., central processing units (CPUs), processors, or controllers.

[0075] As is known in the art, the operations described above can be performed by hardware, software, or some combination of software and hardware. Various aspects of the example implementations may be implemented using circuits and logic devices (hardware), while other aspects may be implemented using instructions stored on a machine-readable medium (software), which if executed by a processor, would cause the processor to perform a method to carry out implementations of the present application. Further, some example implementations of the present application may be performed solely in hardware, whereas other example implementations may be performed solely in software. Moreover, the various functions described can be performed in a single unit, or can be spread across a number of components in any number of ways. When performed by software, the methods may be executed by a processor, such as a general purpose computer, based on instructions stored on a computer-readable medium. If desired, the instructions can be stored on the medium in a compressed and/or encrypted format.

[0076] Moreover, other implementations of the present application will be apparent to those skilled in the art from consideration of the specification and practice of the teachings of the present application. Various aspects and/or components of the described example implementations may be used singly or in any combination. It is intended that the specification and example implementations be considered as examples only, with the true scope and spirit of the present application being indicated by the following claims.

CLAIMS

What is claimed is

1. A system comprising:

one or more first nodes configured to manage a plurality of first blockchains configured to manage transactions for a plurality of applications; and

one or more second nodes configured to manage a second blockchain configured to manage integrity for the plurality of first blockchains;

wherein for an update to one of the plurality of first blockchains, the one or more first nodes are configured to generate key information associated with the one of the first blockchains and provide the key information to the one or more second nodes, wherein the one or more second nodes are configured to store the key information in the second blockchain.

2. The system of claim 1, wherein the key information comprises one or more of a blockchain ledger status of the one of the plurality of first blockchains, network data associated with the one of the plurality of first blockchains, and transaction meta data.

3. The system of claim 1, wherein the key information comprises a hash value of a block of data in the one of the plurality of first block chains associated with a most recent one of the transactions, and a time stamp.

4. The system of claim 1, wherein the one or more second nodes are configured to:

generate propagation data associated with the second blockchain, and transmit the propagation data to the one or more first nodes;

wherein the one or more first nodes are configured to store the propagation data in all of the plurality of first block chains.

5. The system of claim 1, wherein the one or more second nodes are configured to, for receipt of a request comprising index data associated with one of the transactions stored in the plurality of first blockchains:

process the request to locate the one of the transactions in the plurality of first blockchains; and

provide a result of the processing to a client device associated with the request.

6. The system of claim 1, wherein the one or more first nodes are configured to, for a new transaction added to the transactions of the plurality of first blockchains, provide index data to the new transaction in a form of a Quick Release (QR) code indicative of a transaction identifier of the new transaction.

7. A method, comprising:

managing a plurality of first blockchains configured to manage transactions for a plurality of applications on one or more first nodes;

managing a second blockchain configured to manage integrity for the plurality of first blockchains on one or more second nodes;

for an update to one of the plurality of first blockchains, generating key information associated with the one of the first blockchains and storing the key information in the second blockchain.

8. The method of claim 7, wherein the key information comprises one or more of a blockchain ledger status of the one of the plurality of first blockchains, network data associated with the one of the plurality of first blockchains, and transaction meta data.

9. The method of claim 7, wherein the key information comprises a hash value of a block of data in the one of the plurality of first block chains associated with a most recent one of the transactions, and a time stamp.

10. The method of claim 7, further comprising:

generating propagation data associated with the second blockchain, and

storing the propagation data in all of the plurality of first block chains.

11. The method of claim 7, further comprising, for receipt of a request comprising index data associated with one of the transactions stored in the plurality of first blockchains:

processing the request to locate the one of the transactions in the plurality of first blockchains; and

providing a result of the processing to a client device associated with the request.

12. The method of claim 7, further comprising, for a new transaction added to the transactions of the plurality of first blockchains, providing index data to the new transaction in a form of a Quick Release (QR) code indicative of a transaction identifier of the new transaction.

13. A non-transitory computer readable medium, storing instructions for executing a process, the instructions comprising:

managing a plurality of first blockchains configured to manage transactions for a plurality of applications on one or more first nodes;

managing a second blockchain configured to manage integrity for the plurality of first blockchains on one or more second nodes; and

for an update to one of the plurality of first blockchains, generating key information associated with the one of the first blockchains and storing the key information in the second blockchain.

14. The non-transitory computer readable medium of claim 13, wherein the key information comprises one or more of a blockchain ledger status of the one of the plurality of first blockchains, network data associated with the one of the plurality of first blockchains, and transaction meta data.

15. The non-transitory computer readable medium of claim 13, wherein the key information comprises a hash value of a block of data in the one of the plurality of first block chains associated with a most recent one of the transactions, and a time stamp.

16. The non-transitory computer readable medium of claim 13, the instructions further comprising:

generating propagation data associated with the second blockchain, and

storing the propagation data in all of the plurality of first block chains.

17. The non-transitory computer readable medium of claim 13, the instructions further comprising, for receipt of a request comprising index data associated with one of the transactions stored in the plurality of first blockchains:

processing the request to locate the one of the transactions in the plurality of first blockchains; and

providing a result of the processing to a client device associated with the request.

18. The non-transitory computer readable medium of claim 13, further comprising, for a new transaction added to the transactions of the plurality of first blockchains, providing index data to the new transaction in a form of a Quick Release (QR) code indicative of a transaction identifier of the new transaction.

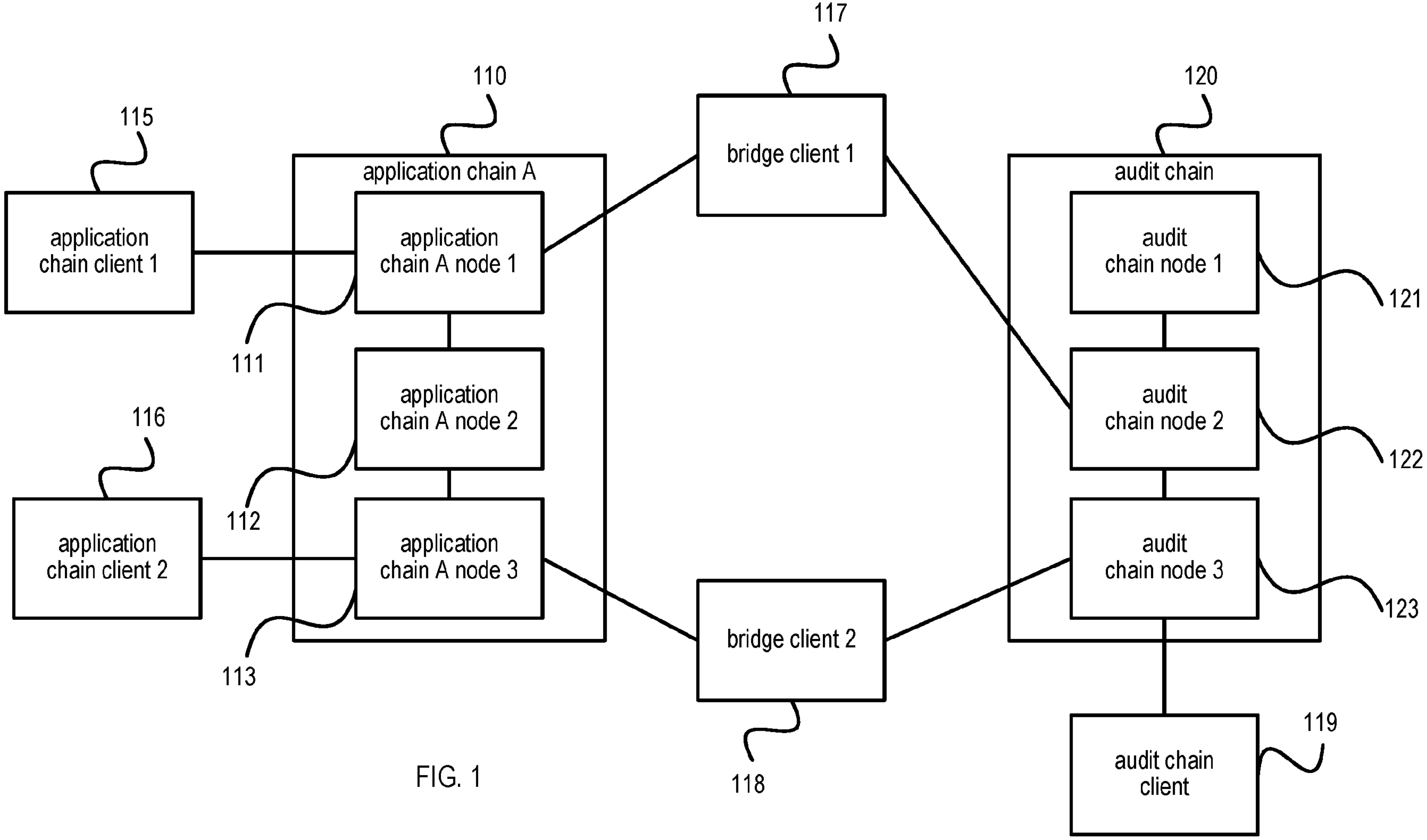

117
110
120
115
application chain A
bridge client 1
audit chain
application chain client 1
application chain A node 1
audit chain node 1
121
111
application chain A node 2
audit chain node 2
116
122
112
application chain client 2
application chain A node 3
audit chain node 3
123
113
bridge client 2
119
audit chain client
118

FIG. 1

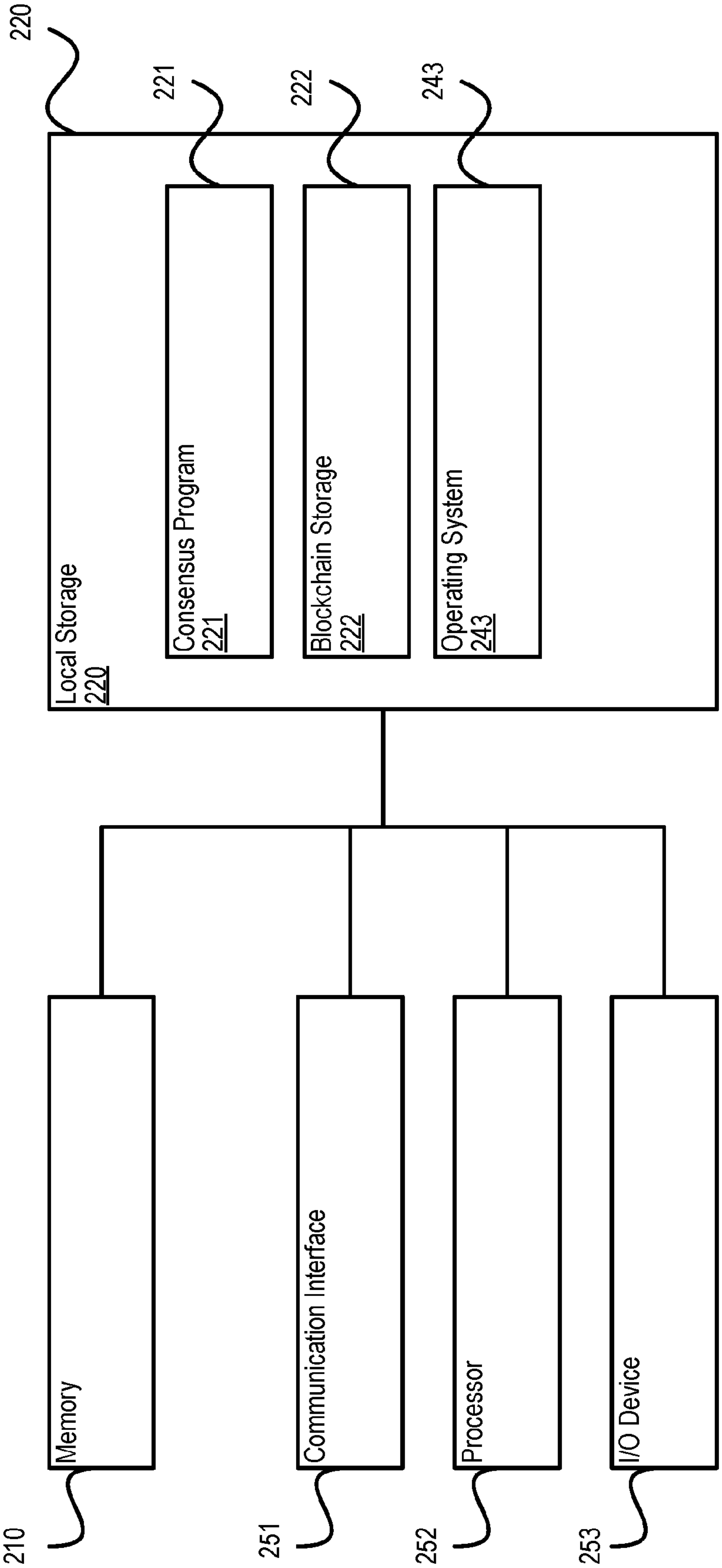
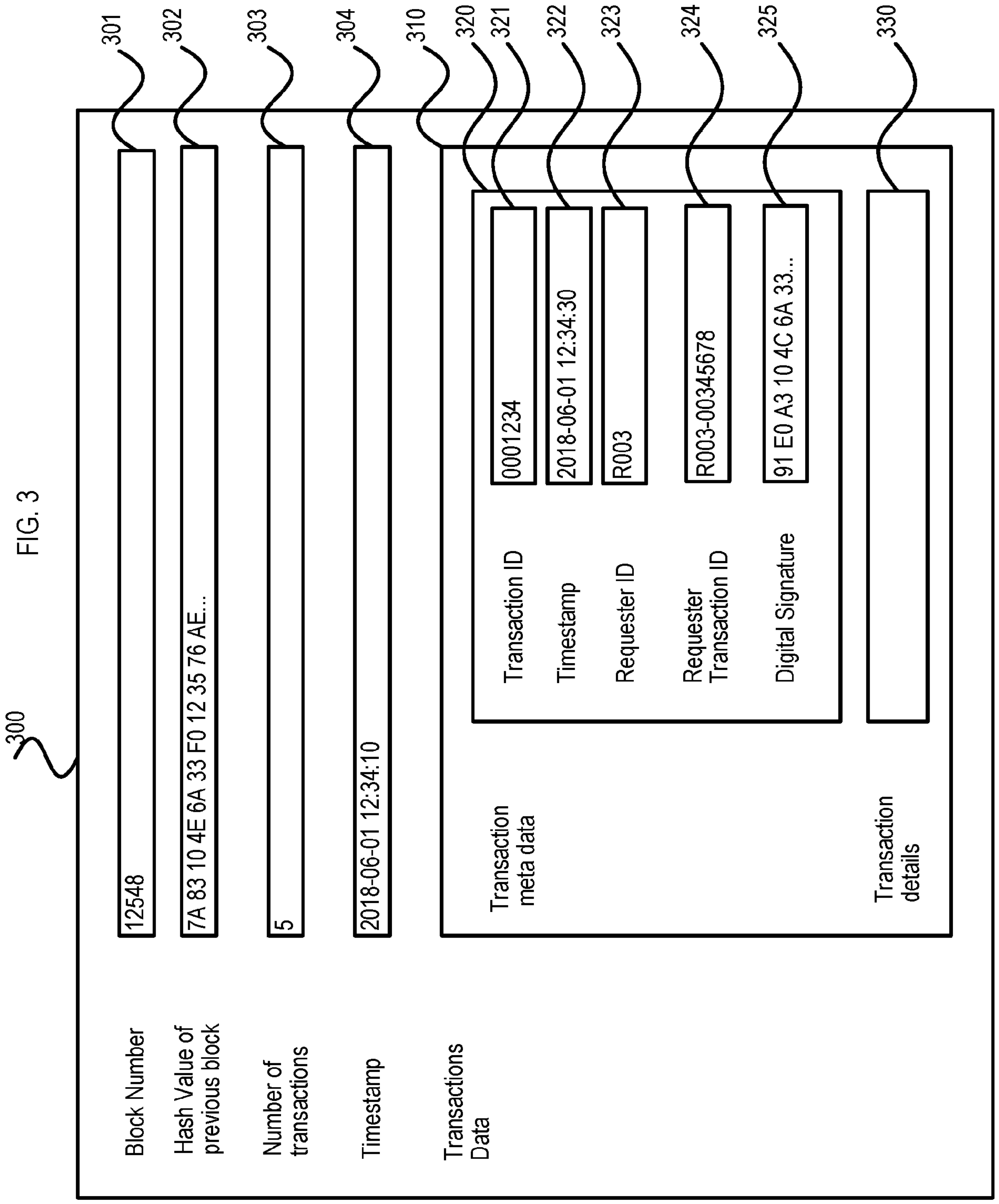

220
221
222
243
Local Storage
220
Consensus Program
221
Blockchain Storage
222
Operating System
243
Memory
Communication Interface
Processor
I/O Device
210
251
252
253

FIG. 2

FIG. 3


300
301
302
303
304
310
320
321
322
323
324
325
330
Block Number
12548
Hash Value of previous block
7A 83 10 4E 6A 33 F0 12 35 76 AE...
Number of transactions
5
Timestamp
2018-06-01 12:34:10
Transactions Data
Transaction meta data
Transaction ID
0001234
Timestamp
2018-06-01 12:34:30
Requester ID
R003
Requester Transaction ID
R003-00345678
Digital Signature
91 E0 A3 10 4C 6A 33...
Transaction details

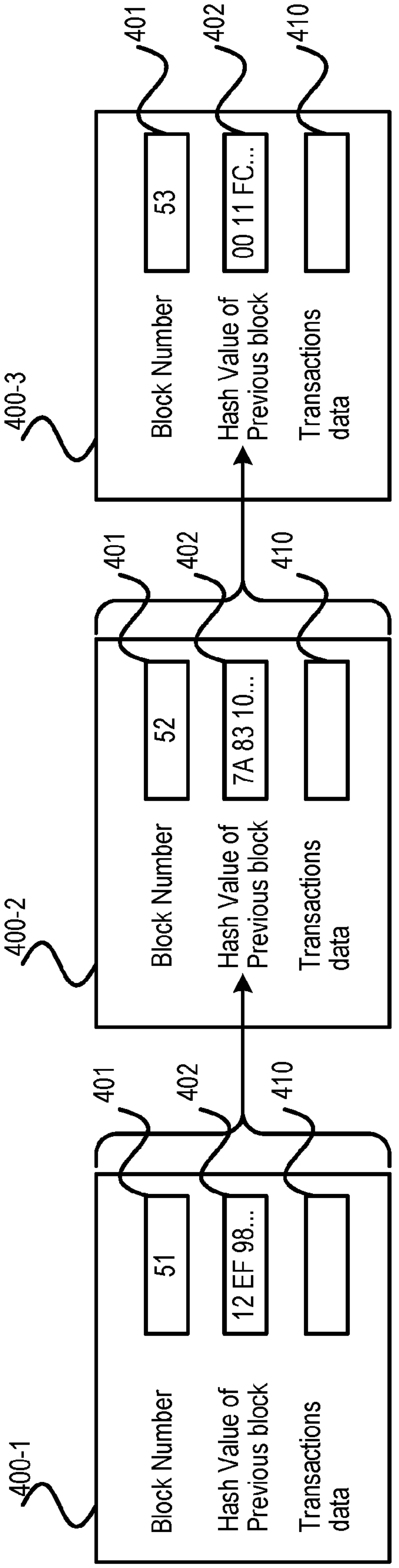

400-1
Block Number
51
Hash Value of Previous block
12 EF 98...
Transactions data
401
402
410
400-2
Block Number
52
Hash Value of Previous block
7A 83 10...
Transactions data
401
402
410
400-3
Block Number
53
Hash Value of Previous block
00 11 FC...
Transactions data
401
402
410

FIG. 4

FIG. 5

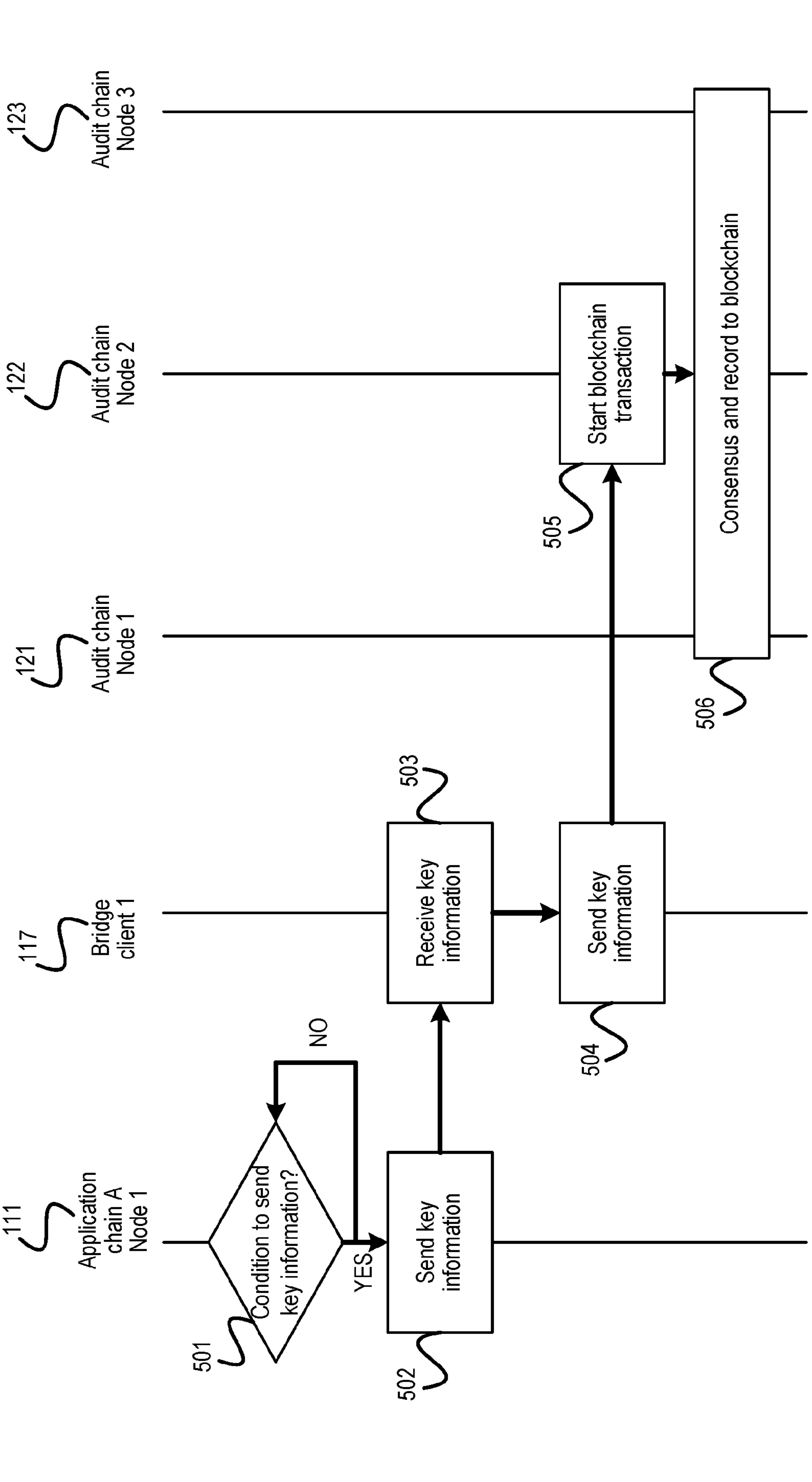
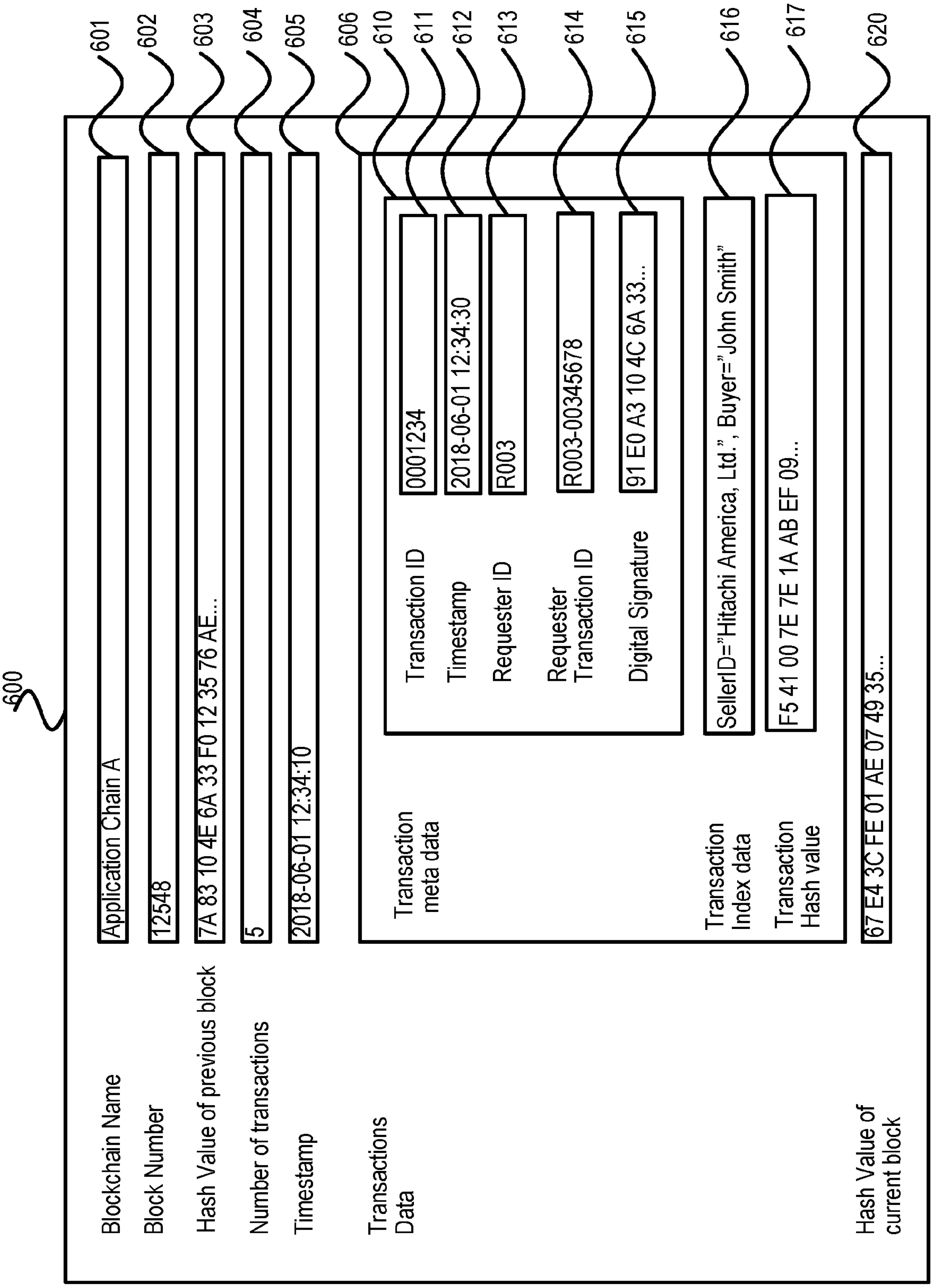

111
Application chain A Node 1
117
Bridge client 1
121
Audit chain Node 1
122
Audit chain Node 2
123
Audit chain Node 3
501
Condition to send key information?
NO
YES
502
Send key information
503
Receive key information
504
Send key information
505
Start blockchain transaction
506
Consensus and record to blockchain

FIG. 6


600
601
602
603
604
605
606
610
611
612
613
614
615
616
617
620
Blockchain Name
Application Chain A
Block Number
12548
Hash Value of previous block
7A 83 10 4E 6A 33 F0 12 35 76 AE…
Number of transactions
5
Timestamp
2018-06-01 12:34:10
Transactions Data
Transaction meta data
Transaction ID
0001234
Timestamp
2018-06-01 12:34:30
Requester ID
R003
Requester Transaction ID
R003-00345678
Digital Signature
91 E0 A3 10 4C 6A 33…
Transaction Index data
SellerID="Hitachi America, Ltd.", Buyer="John Smith"
Transaction Hash value
F5 41 00 7E 7E 1A AB EF 09…
Hash Value of current block
67 E4 3C FE 01 AE 07 49 35…

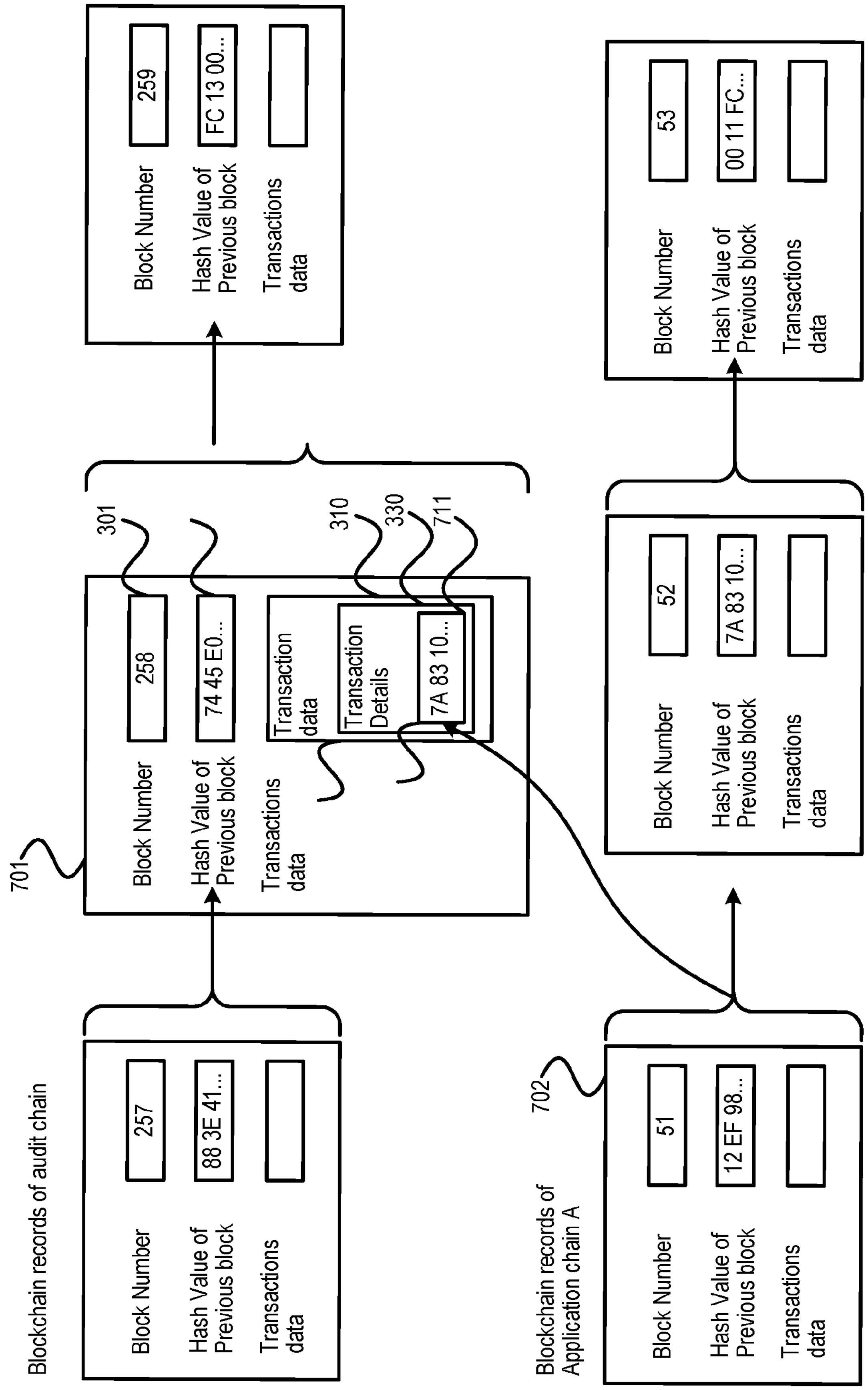

Blockchain records of audit chain
Block Number
257
Hash Value of Previous block
88 3E 41...
Transactions data
701
Block Number
258
Hash Value of Previous block
74 45 E0...
Transactions data
Transaction data
Transaction Details
7A 83 10...
301
310
330
711
Block Number
259
Hash Value of Previous block
FC 13 00...
Transactions data
Blockchain records of Application chain A
702
Block Number
51
Hash Value of Previous block
12 EF 98...
Transactions data
Block Number
52
Hash Value of Previous block
7A 83 10...
Transactions data
Block Number
53
Hash Value of Previous block
00 11 FC...
Transactions data

FIG. 7

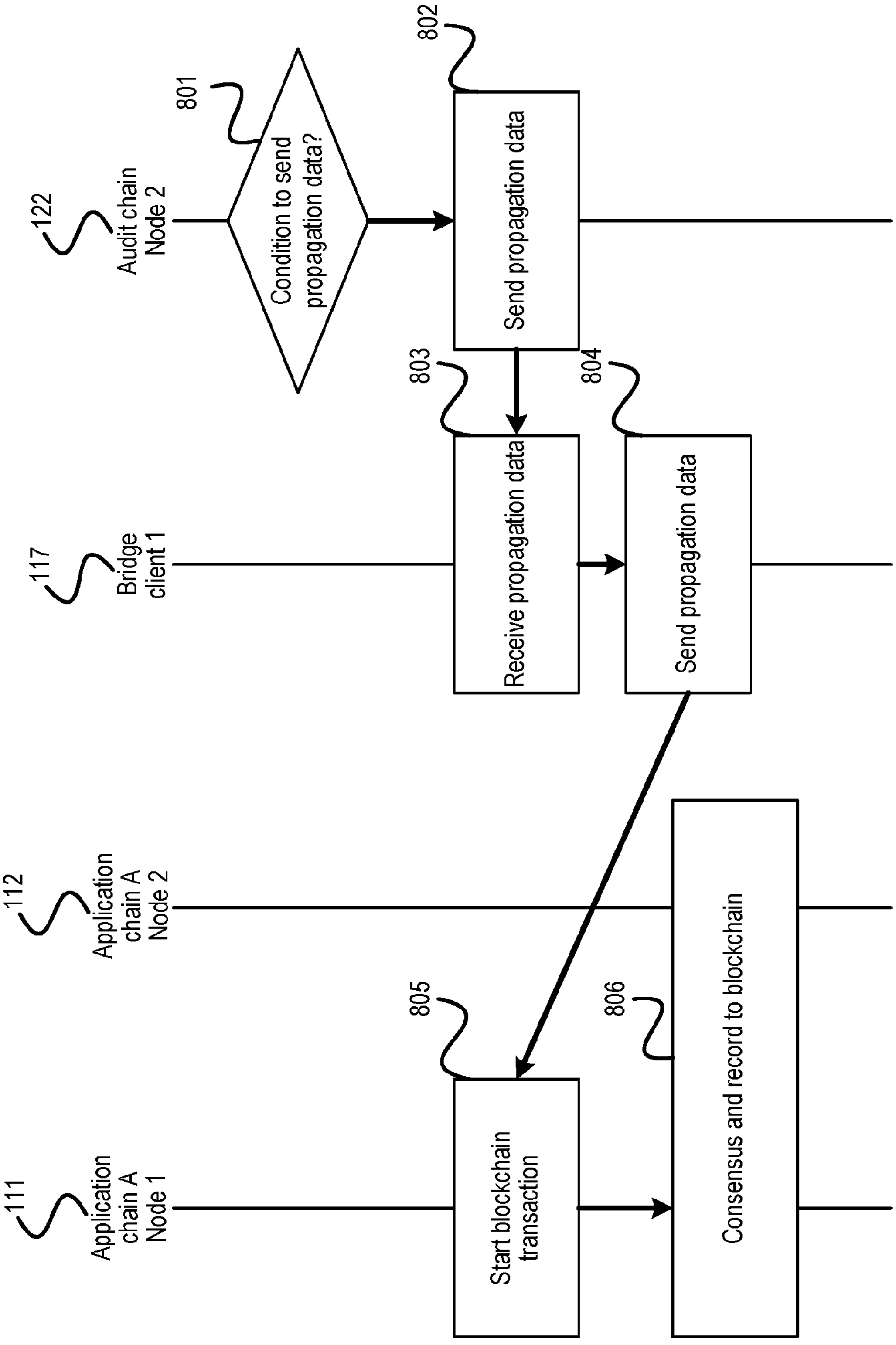
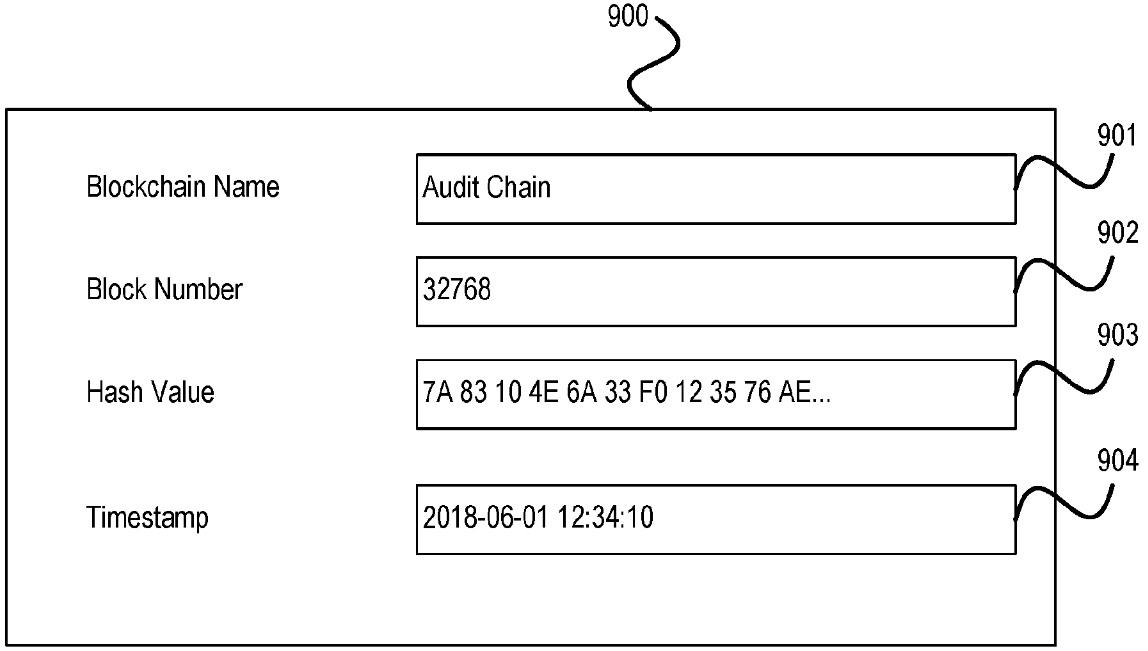

122
Audit chain Node 2
801
Condition to send propagation data?
802
Send propagation data
117
Bridge client 1
803
Receive propagation data
804
Send propagation data
112
Application chain A Node 2
111
Application chain A Node 1
805
Start blockchain transaction
806
Consensus and record to blockchain

FIG. 8



Blockchain Name: Audit Chain

Block Number: 32768

Hash Value: 7A 83 10 4E 6A 33 F0 12 35 76 AE...

Timestamp: 2018-06-01 12:34:10

FIG. 9

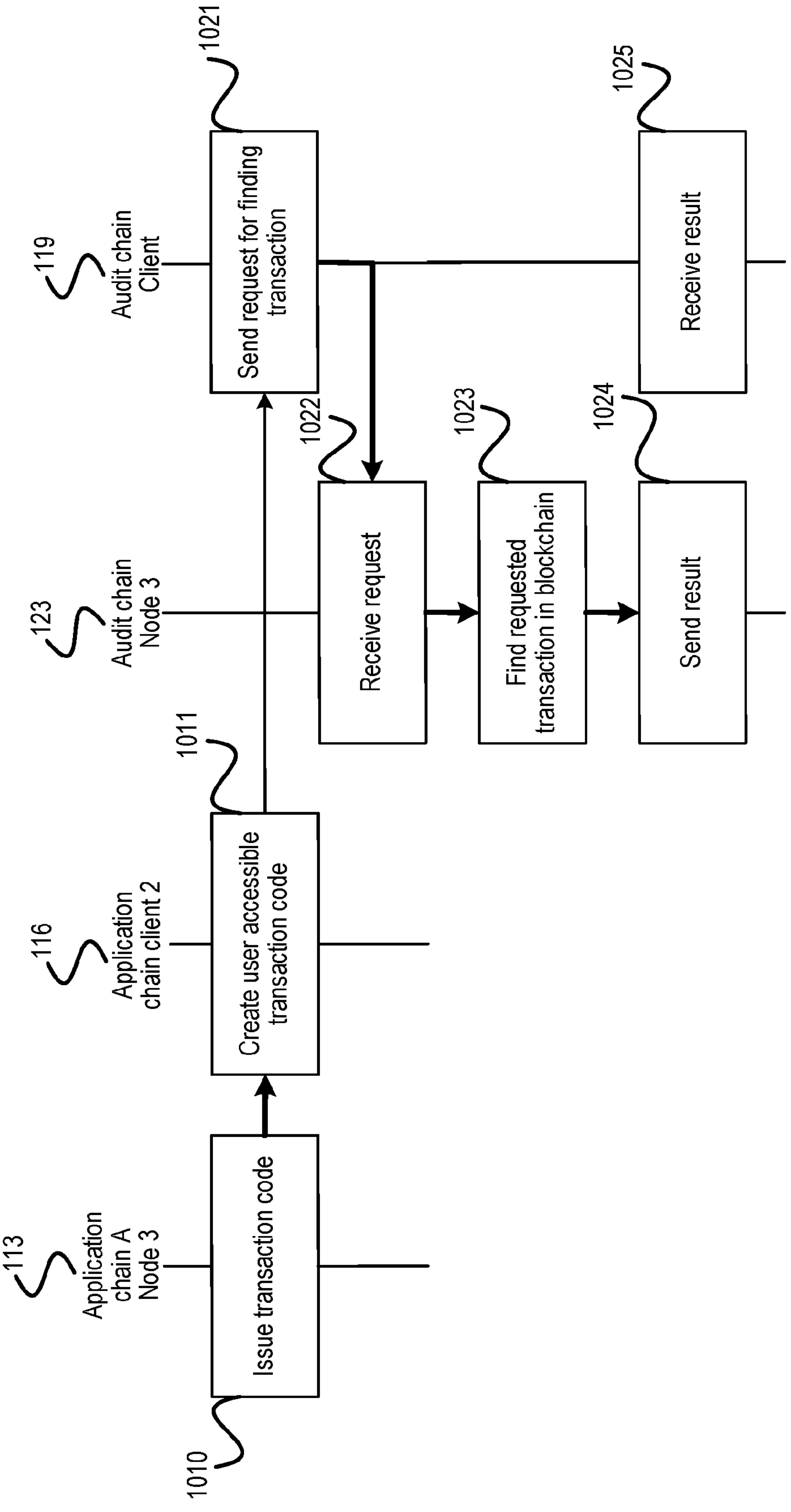

Application chain A Node 3
113
Issue transaction code
1010
Application chain client 2
116
Create user accessible transaction code
1011
Audit chain Node 3
123
Receive request
1022
Find requested transaction in blockchain
1023
Send result
1024
Audit chain Client
119
Send request for finding transaction
1021
Receive result
1025

FIG. 10

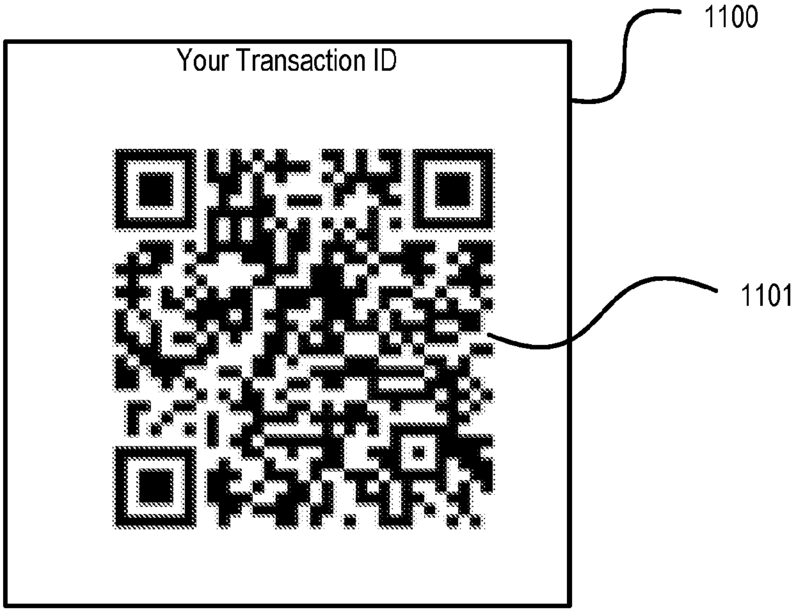


FIG. 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 18/50963

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - H04L 9/32 (2018.01)
CPC - H04L 9/3247, H04L 9/3066, H04L 2209/38, H04L 9/3249, H04L 9/3252

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)
See Search History Document

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Catcgory*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X ---- Y	US 2017/0046638 A1 (TD Bank Group) 16 February 2017 (16.02.2017) (para [0006]-[0008], [0076], [0136], [0142], [0149]-[0151], [0153]-[0156], [0162]-[0167], [0193], [0203]-[0206])	1-5, 7-11, and 13-17 ---------------------------- 6, 12, 18
Y	US 2017/0237554 A1 (Jacobs et al.) 17 August 2017 (17.08.2017) (para [0159])	6, 12, 18
A	US 2016/0328713 A1 (ShoCard, Inc.) 10 November 2016 (10.11.2016) entire document	1-18

□ 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
"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 20 November 2018	Date of mailing of the international search report 07 DEC 2018
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774