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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
08 July 2021 (08.07.2021)

WIPO | PCT

(10) International Publication Number
WO 2021/134835 A1

(51) International Patent Classification:
H04L 29/06 (2006.01)

(21) International Application Number:
PCT/CN2020/071953

(22) International Filing Date:
14 January 2020 (14.01.2020)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
16/732,867 02 January 2020 (02.01.2020) US

(71) Applicant: **HONG KONG APPLIED SCIENCE AND TECHNOLOGY RESEARCH INSTITUTE COMPANY LIMITED** [CN/CN]; 5/F, Photonics Centre, 2 Science Park East Avenue, Hong Kong Science Park, Shatin, N.T., Hong Kong (CN).

(72) Inventors: **LAM, Tak Wing**; 2A Waterloo Heights Garden, 3 Man Wan Road, Kowloon, Hong Kong (CN). **YEUNG, Kai Wah**; Flat 1401, Hong Ting House, Hong Yat Court, Lam Tin, Hong Kong (CN). **WONG, Tak Fuk**; Rm 4013, Yeung Shue Hse, Lei Muk Shue Est, Kwai Chung, N.T., Hong Kong (CN).

(74) Agent: **CHINA TRUER IP**; Room 401, Floor 4, Zhongdian Difu Building, Zhenhua Road, Fuqiang Community, Huaqiang North Street, Futian District, Shenzhen, Guangdong 518031 (CN).

(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,

(54) Title: SYSTEM AND METHODS FOR DATA EXCHANGE USING A DISTRIBUTED LEDGER

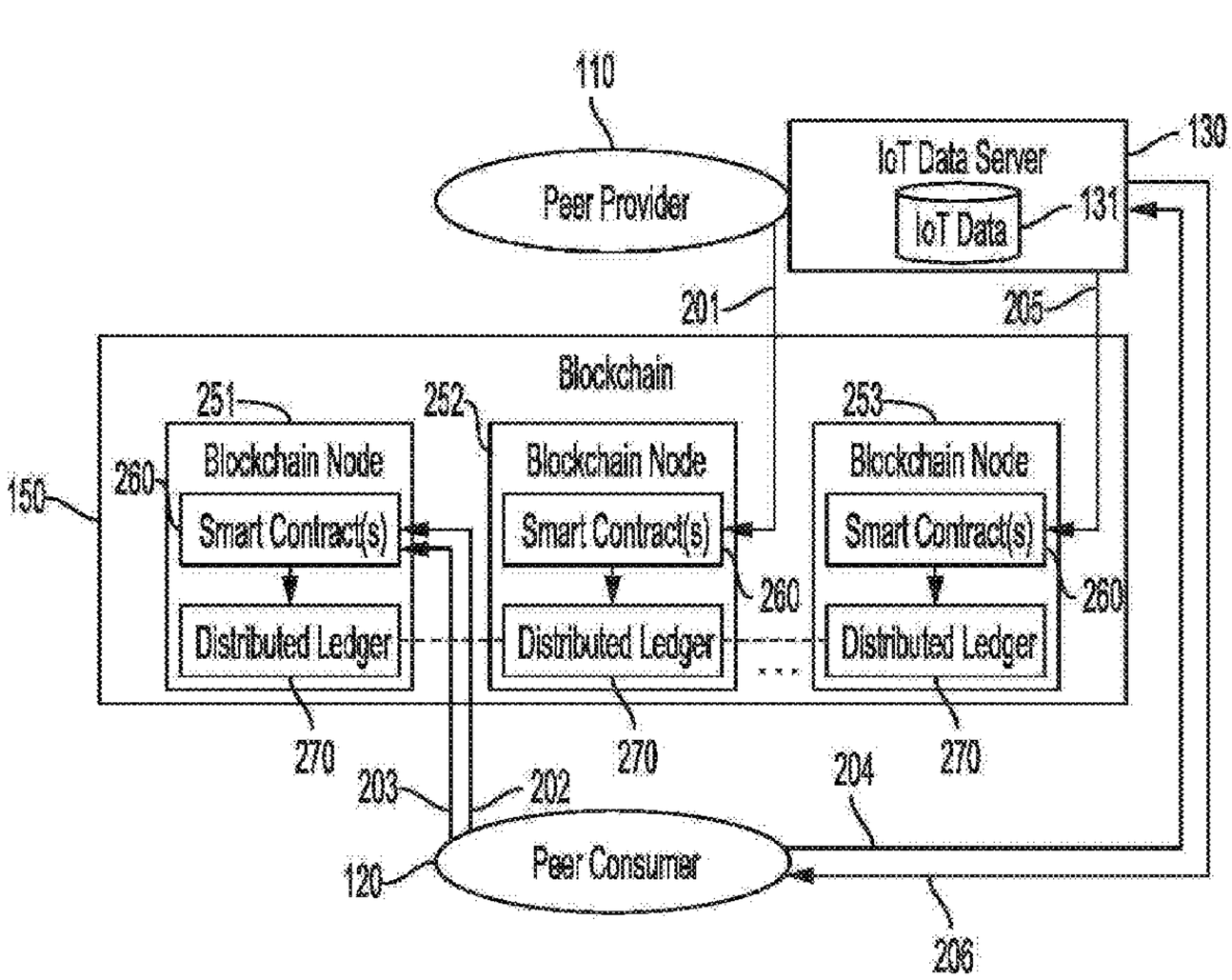

FIG. 2

(57) Abstract: Systems and methods which provide data exchange using a distributed ledger, wherein data is exchanged off-chain and information for accessing the off-chain data is exchanged through the blockchain, are disclosed. Embodiments may provide a hybrid blockchain data exchange platform storing large amounts of data (e.g., IoT data) in a data server outside of the blockchain, wherein a data consumer may obtain data from the data server using a token obtained from the blockchain. Embodiments of a hybrid blockchain data exchange platform provide for accuracy and security of the data without requiring storage of the full contents of the data within the blockchain, and/or provide data exchange in which the irrefutability of the data exchanged is ensured.

[Continued on next page]

WO 2021/134835 A1

SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, 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, 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).

Published:

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

SYSTEM AND METHODS FOR DATA EXCHANGE USING A DISTRIBUTED LEDGER

TECHNICAL FIELD

[0001] The present invention relates generally to data exchange between a data provider and a data consumer and, more particularly, to data exchange using a distributed ledger.

BACKGROUND OF THE INVENTION

[0002] The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. With the widespread adoption of connected devices, such as smart appliances, cameras, voice controlled personal assistants, smartphones, sensors, etc., the IoT system is becoming widely used. Accordingly, a large amount of IoT data (e.g., sensor data, captured video and/or audio, transaction data, etc.) is being generated. Such diverse and robust IoT data may be utilized by a number of data consumers (e.g., individuals, commercial enterprises, governmental departments, researchers, security forces, and/or the like) for various purposes (e.g., identifying needs to be served, determining eligibility for special offers, targeting advertising and other marketing efforts, identifying behaviors and trends, identifying security threats, etc.). However, the sheer volume of available IoT data and its diverse sources can prove challenging for a data consumer to identify relevant available IoT data, to determine a location from which relevant IoT data is available, and to access and obtain specific IoT data.

[0003] Moving the IoT data into a decentralized path can provide advantages with respect to avoiding single point of failure and facilitating widespread data discovery and access. Blockchain is one relatively recent technology which has become popular in implementing decentralization systems.

[0004] Blockchain technology provides for data to be distributed throughout a network of storage nodes (i.e., blockchain network) and securely stored in a digital or distributed ledger. In operation of a blockchain, a growing list of blocks (ledger) which are linked using cryptography are generated and maintained. Each block contains a cryptographic hash of the previous block (hash, transaction data, etc.). Each node in blockchain network has a copy of the ledger, thereby providing a distributed ledger. A consensus mechanism (e.g., proof of work) maintains synchronization with respect to all of the ledgers. In a permissioned private blockchain, only authorized participants can join the network, and read and commit a transaction (e.g., useful for enterprise applications, allowing only trusted nodes to participate in the blockchain operation). Permissioned private blockchains generally allow for high scalability (e.g., Hyperledger can achieve 3500 transactions per second). In a permissionless public blockchain, anyone can join the network, read, write and commit a transaction (e.g., useful for cryptocurrency applications, allowing anyone to participate in the blockchain operation). Permissionless public blockchains generally provide low scalability (e.g., Bitcoin requires around 10 minutes to confirm a single transaction).

[0005] Blockchain can provide a powerful technology that decentralizes computation and management processes which can solve many IoT data issues (e.g., data security, discoverability, and access). However, practical implementation of blockchain technology for storage of and access to IoT data is itself challenging. For example, blockchain distributed ledgers utilize appreciable computing resources in generating the chained blocks of data stored by each node of the blockchain network. IoT data presents a tremendous amount of data which, if the IoT data management platforms merely store the IoT data to a blockchain, may prove impractical. For example, performing raw IoT data transaction on-chain may not be favorable in light of the tremendous amount of IoT data involved. The transaction speed available with respect to IoT data transactions implemented on-chain is likely to be unacceptably low due to the consensus protocol implemented by the blockchain. Moreover, every node in the blockchain would have a copy of the distributed ledger, including every transaction on the IoT data, and thus may consume a tremendous amount of

storage space. Accordingly, the blockchain is likely to have issues with respect to long processing times and requiring large blockchain storage space if tasked with storing IoT data.

[0006] Some prior attempts at moving IoT data into a decentralized path include the IoT data management platform have been made. For example, CN108694330A, the disclosure of which is incorporated herein by reference, discloses an IoT data management platform in which a node in a blockchain network receives the IoT data and determines data validity. The valid data will be written into the blockchain network. The node in a blockchain network also receives operation instruction and determines its validity. Data service is generated if the operation instruction is valid. US10,264,066B2, the disclosure of which is incorporated herein by reference, discloses a technique for peer-to-peer (P2P) data sharing among IoT networks. In particular, the techniques therein provide for data sharing between two IoT platforms through P2P connection involving a security token. US2019/0165945A1, the disclosure of which is incorporated herein by reference, discloses a multi-node transaction management system to generate one-time token for a group of client nodes with help of a blockchain platform. None of these prior attempts, however, address issues with respect to long processing times and large blockchain storage space as may be presented by IoT data.

BRIEF SUMMARY OF THE INVENTION

[0007] The present invention is directed to systems and methods which provide data exchange using a distributed ledger, wherein data is exchanged off-chain and information for accessing the off-chain data is exchanged through the blockchain. Embodiments of the present invention provide a hybrid blockchain implementation that avoids storing the bulk of the data within the blockchain, thus providing solutions well suited for data exchange with respect to very large volumes of data (e.g., IoT data). Embodiments facilitate data exchange with respect to large amounts of data using a blockchain system, enabling the data exchange in an efficient manner while preserving data accuracy and security.

[0008] Embodiments of the present invention may, for example, provide a hybrid blockchain data exchange platform storing large amounts of data (e.g., IoT data) in one or more data servers outside of the blockchain. This data may be made available (e.g., "published") by a data provider to data consumers by registering the data (e.g., as a data service) to the blockchain. A data consumer may access the distributed ledger of the blockchain to discover relevant data or data of interest and obtain a data token (e.g., data service token) from the blockchain for use in obtaining data from the one or more data servers. Thereafter, the data consumer may access or otherwise obtain data from one or more data servers using the token obtained from the blockchain. Such a hybrid blockchain implementation facilitates widespread discovery of and access to large amounts of data while avoiding issues with respect to long processing times and large blockchain storage space.

[0009] Embodiments of a hybrid blockchain data exchange platform of embodiments provide for accuracy and security of the data without requiring storage of the full contents of the data within the blockchain. For example, a data structure (e.g., Bloom filter) representative of the data may be stored by the blockchain and used in verifying the integrity of data obtained from one or more data servers of the hybrid blockchain data exchange platform. Representative data structures of embodiments utilize significantly less blockchain storage space than would storage of the data itself within the blockchain, while nevertheless facilitating data security and assurance of data accuracy.

[0010] Hybrid blockchain data exchange platforms of embodiments of the invention provide data exchange in which the irrefutability of the data exchanged is ensured. For example, the data obtained by a data consumer from a data server of the hybrid blockchain data exchange platform may be encrypted, wherein information (e.g., representative data structure, such as hash value, and decryption key) for extracting the data is stored within the blockchain by the data provider. The

data consumer may obtain the information from extracting the data from the blockchain, thus confirming receipt of the data.

[0011] The foregoing has outlined rather broadly the features and technical advantages of the present invention in order that the detailed description of the invention that follows may be better understood. Additional features and advantages of the invention will be described hereinafter which form the subject of the claims of the invention. It should be appreciated by those skilled in the art that the conception and specific embodiment disclosed may be readily utilized as a basis for modifying or designing other structures for carrying out the same purposes of the present invention. It should also be realized by those skilled in the art that such equivalent constructions do not depart from the spirit and scope of the invention as set forth in the appended claims. The novel features which are believed to be characteristic of the invention, both as to its organization and method of operation, together with further objects and advantages will be better understood from the following description when considered in connection with the accompanying figures. It is to be expressly understood, however, that each of the figures is provided for the purpose of illustration and description only and is not intended as a definition of the limits of the present invention.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] For a more complete understanding of the present disclosure, reference is now made to the following descriptions taken in conjunction with the accompanying drawings, in which:

[0013] FIGURE 1 shows a high level functional block diagram of a hybrid blockchain data exchange platform according to embodiments of the present invention;

[0014] FIGURE 2 shows further detail with respect to the operation of hybrid blockchain data exchange platform of FIGURE 1;

[0015] FIGURE 3 shows a flow diagram setting forth a functional flow of operation by a hybrid blockchain data exchange platform to provide data exchange according to embodiments of the present invention;

[0016] FIGURES 4A and 4B show flow diagrams setting forth a functional flow for verification of the integrity of data of IoT data according to embodiments of the present invention; and

[0017] FIGURES 5A and 5B show flow diagrams setting forth a functional flow for ensuring the irrefutability of the data exchanged according to embodiments of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0018] FIGURE 1 shows a high level functional block diagram of a hybrid blockchain data exchange platform configured to provide data exchange in accordance with concepts of the present invention. In operation of hybrid blockchain data exchange platform 100, data is exchanged off-chain and information for accessing the off-chain data is exchanged through the blockchain. Accordingly, hybrid blockchain data exchange platform 100 avoids storing the bulk of the data within the blockchain, and thus is well suited for facilitating data exchange with respect to very large volumes of data (e.g., IoT data).

[0019] In the example of hybrid blockchain data exchange platform 100 shown in FIGURE 1 is configured for storing large amounts of data (e.g., IoT data 131) in one or more data servers, such as IoT data server 130, outside of the blockchain. This data may be made available by peer provider 110 to peer consumer 120 using blockchain 150, as described in further detail below. It should be appreciated that, although only one instance of a peer provider, peer consumer, IoT data server, and blockchain is shown in FIGURE 1 for simplifying the illustration, a hybrid blockchain data exchange platform operable according to concepts of the present invention may include different numbers of any or all of the foregoing. For example, it is expected that a plurality of data consumers will access data of any particular data provider. Moreover, it is expected that a plurality

of data providers will participate with respect to an implementation of a hybrid blockchain data exchange platform.

[0020] Peer provider 110 of the exemplary embodiment in FIGURE 1 may, for example, comprise one or more systems of a source of IoT data (e.g., systems of an owner, operator, aggregator, etc. with respect to connected devices, such as smart appliances, cameras, voice controlled personal assistants, smartphones, sensors, drones, etc.) operable to generate, obtain, collect, aggregate, mange, or otherwise facilitate access to IoT data. Correspondingly, peer consumer 120 may, for example, comprise one or more systems of a consumer of IoT data (e.g., systems of an individual, commercial enterprise, governmental department, researcher, security force, etc.) operable to access, obtain, utilize, analyze, consume, or otherwise facilitate accessing IoT data for various purposes (e.g., identifying needs to be served, determining eligibility for special offers, targeting advertising and other marketing efforts, identifying behaviors and trends, identifying security threats, etc.). In accordance with some embodiments, peer provider 110 and/or peer consumer 120 may comprise one or more processor-based systems (e.g., personal computer or other computer implementation, web server or other server implementation, smartphone, tablet device, etc.) operating under control of instructions (e.g., program code) defining operation as described herein. For example, peer provider 110 and/or peer consumer 120 may comprise a central processing unit (CPU) in communication with computer readable memory storing program code which, when executed by the CPU, performs functions described herein.

[0021] IoT data server 130 of the exemplary embodiment in FIGURE 1 provides a platform for collecting and serving IoT data 131. IoT data server 130 may, for example, comprise one or more data servers (e.g., web server or other server configuration, storage area network (SAN), redundant array of inexpensive disks (RAID) array, etc.) operable to store IoT data 131 provided by one or more data providers (e.g., peer provider 110). In accordance with some embodiments of the invention, IoT data sever 130 may be operated by, controlled by, or otherwise associated with peer provider 110 for storing IoT data provided by a data provider corresponding to peer provider 110. IoT data server 130 may be in data communication with one or more systems of peer provider 110 via a network, such as a local area network (LAN), a wide area network (WAN), the Internet, an intranet, a cellular communication network, etc., for receiving IoT data and associated information (e.g., data tokens, representative data structures, cryptographic keys, digital certificates/signatures, etc.), such as for storage, for management, maintenance, and control operations, etc. IoT data server 130 is preferably accessible to one or more systems peer consumer 120 via a network, such as a LAN, WAN, the Internet, an intranet, a cellular communication network, etc., for providing access to some or all of the IoT data and associated information (e.g., data tokens, representative data structures, cryptographic keys, digital certificates/signatures, etc.), such as for facilitating IoT data exchange with the peer consumer. In accordance with some embodiments, IoT data server 130 may comprise one or more processor-based systems (e.g., personal computer or other computer implementation, web server or other server implementation, smartphone, tablet device, etc.) operating under control of instructions (e.g., program code) defining operation as described herein. For example, IoT data server 130 may comprise a CPU in communication with computer readable memory storing program code which, when executed by the CPU, performs functions described herein.

[0022] Blockchain 150 of embodiments comprises a network of nodes operating cooperatively to form a permissioned private blockchain network. The blockchain system implemented as blockchain 150 is configured to support smart contracts. The smart contracts comprise computer code stored on blockchain 150 containing predetermined rules, wherein when rules are met, the code will be executed. Accordingly, blockchain 150 is operable to perform credible transactions without the help of third parties. Different roles and smart contracts may, for example, be pre-defined by a network administrator or other manager to address various needs, such as roles of peer provider (e.g., IoT data provider) and peer consumer (e.g., IoT data consumer) and smart contracts providing rules and associated code for implementing functions of the hybrid blockchain data exchange platform. Some exemplary smart contracts as may be utilized in

implementing embodiments of hybrid blockchain data exchange platform are set forth in the table below.

	Smart Contract Input Parameters	Record Created in Ledger	Return Values of Smart Contract
(SC1) Smart Contract for IoT Data Service Registration (for peer_provider only)	• **Identity** of participant who invokes the contract • **Data filtering parameters:** data type, valid time, etc • Data **access methods** (rest, MQTT, etc.)	• **Identity** of participant who invokes the contract • **Data filtering parameters:** data type, valid time, etc • Data **access methods** (rest, MQTT, etc.) • **Data uuid** of the record	• **Data uuid** of the record

	{
	peer_identity : "peer_provider",
	data_filtering_parameters: ["Location", "20191201,12pm – 1pm"],
	data_access_methods: ["rest api"]
	}
		{
		peer_identity : "peer_provider",
		data_filtering_parameters: ["Location", "20191001,12pm – 1pm"],
		data_access_methods : ["rest api"],
		data_uuid : data_101 }
			{
			data_uuid : data_101
			}

(SC2) Smart Contract for IoT Data Service Discovery (for peer_consumer only)	• **Identity** of participant who invokes the contract • **Data filtering parameters:** data type, valid time, etc	Read Operation, no block created	• **All record created by** Smart Contract for IoT Data Service Registration (filtered by filtering parameters)

	{
	peer_identity : "peer_consumer",
	data_filtering_parameters: ["Location"]
	}
		Read Operation, no block created	{
			peer_identity : "peer_provider",
			data_filtering_parameters: ["Location", "20191001,12pm – 1pm"]
			data_access_methods: ["rest api"],
			data_uuid : data_101 }
			……

(SC3) Smart Contract for Requesting Data Access Secret (for peer_consumer only)	• **Identity** of participant who invokes the contract • **Data uuid** of the data to be accessed • **Data filtering parameters:** data type, valid time, etc	• **Identity** of participant who invokes the contract • **Data uuid** of the record • **Nonce** (random number) • **Secret:** hash value of data_access_secret and nonce	• **data_access_secret**
	{ peer_identity : "peer_consumer",	{ peer_identity : "peer_consumer",	{ data_access_secret : "data_access_secret"

	data_uuid : data_101, data_filtering_parameters: xxx }	data_uuid : data_101, nonce : nonce secret : hash("data_access_secret", nonce) }	}
(SC4) Smart Contract for validity of the data_access_secret checking (peer_provider only)	• **Identity** of participant who invokes the contract • **Data Uuid** of the data to be accessed • **Data_access_secret_provided**	Read Operation, no block created	• **Validity**
	{ peer_identity : "peer_provider", data_uuid : data_101 data_access_secret_provided : "xxxxxxxxxx" }	Read Operation, no block created	** check if secret = hash("**data_access_secret_provided**", nonce) if data_access_secret is valid, return 1**
(SC5) Smart Contract for bloom value saving (peer_provider only)	• **Identity** of participant who invokes the contract • **Bloom Filter**	• **Identity** of participant who invokes the contract • **Bloom value** • **bloom uuid** of the record	• **bloom uuid** of the record
	{ peer_identity: "peer_provider", bloom_filter : bloom_filter }	{ peer_identity : "peer_provider", bloom_filter : bloom_filter, **bloom_filter_uuid** : bloom_101 }	{ **bloom_filter_uuid** : bloom_101 }
(SC6) Smart Contract for validity checking (peer_consumer only)	• **Identity** of participant who invokes the contract • **Hash value of data** • **Bloom uuid of the record**	Read Operation, no block created	• validity
	{ peer_id : "peer_consumer", hash_data : Hash(data_x), bloom_uuid : bloom_101 }	Read Operation, no block created	{ validity: 1/0 } *** Test if Hash(data_x) is an element using bloom_filter in **(b)**, if yes, return 1 ***
(SC7) Smart Contract for Encryption Parameters Saving (peer_provider	• **Identity** of participant who invokes the contract • **Hash value of encrypted data** • **Encryption key**	• **Identity** of participant who invokes the contract • **Hash value of encrypted data** • **Encryption key**	• Status of the request: 1 : transaction committed 2 : failed to commit

only)	{ peer_id : "peer_provider", hash_value: hash_value, key : key }	{ peer_id : "peer_provider", hash_value: hash_value, key : key }	{ Status: 1/0 }
(SC8) Smart Contract for Decryption Key Request (peer_consumer only)	• **Identity** of participant who invokes the contract • **Hash value of encrypted data** { peer_id : "peer_consumer", hash_value: hash_value, }	• **Identity** of participant who invokes the contract • **Hash value of encrypted data** { peer_id : "peer_consumer", hash_value: hash_value, }	**Key** of the decryption key { key: key }

[0023] Hybrid blockchain data exchange platform 100 is configured for facilitating data exchange with respect to a large body of data (e.g., IoT data) using blockchain technology. In operation of hybrid blockchain data exchange platform 100 shown in FIGURE 1, data may be made available (e.g., "published") for access by peer consumer 120 by peer provider 110 registering the data (e.g., as a data service) to blockchain 150. Thereafter, peer consumer 120 may access the distributed ledger of blockchain 150 to discover relevant data or data of interest and obtain a data token (e.g., security token, such as a digital signature) from the blockchain for use in obtaining data from IoT data server 130. Peer consumer 120 may thus access or otherwise obtain some portion of IoT data 131 from IoT data server 130 using the token obtained from blockchain 150. As can be appreciated from the foregoing, data of IoT data 131 is exchanged off-chain (i.e., raw, or full/complete, IoT data is neither stored nor directly provided by blockchain 150), whereas information (e.g., data tokens) for accessing relevant data of IoT data 131 is exchanged through blockchain 150.

[0024] FIGURE 2 shows further detail with respect to the operation of hybrid blockchain data exchange platform 100 described above, according to embodiments. In particular, FIGURE 2 provides a logical flow diagram of operation according to embodiments of hybrid blockchain data exchange platform 100. A flow diagram setting forth a functional flow corresponding to the logical flow of FIGURE 2 is shown in FIGURE 3 as flow 300. As described above with respect to the operation of hybrid blockchain data exchange platform 100, operation according to the flows of FIGURES 2 and 3 provides for exchanging data off-chain, wherein raw IoT data is not stored in distributed ledger 270, as described in detail below.

[0025] Hybrid blockchain data exchange platform 100 of embodiments of the invention implements a procedure for peer provider 110 to register data and for peer consumer 120 to discover the data. Accordingly, at block 301 of flow 300, peer provider 110 registers a data service corresponding to data of IoT data 131 using blockchain 150, as illustrated by arrow 201 in FIGURE 2. In accordance with embodiments, peer provider 110 may invoke a smart contract of smart contracts 260 (e.g., smart contract SC1 of the examples above) to register an IoT data service. Registration of the data service may include specifying various attributes for the data, its storage, and access. For example, peer provider 110 may specify various data filtering parameters (e.g., data type, valid time, etc.), data access methods (e.g., rest, MQTT, etc.), and/or the like. Correspondingly, peer provider 110 may store IoT data 131 to IoT data server 130, or otherwise control IoT data server 130 to collect IoT data 131 for serving to data consumers in accordance with the registered data service.

[0026] At block 302 of flow 300, peer consumer 120 discovers the IoT data service using blockchain 150, as illustrated by arrow 202 in FIGURE 2. In accordance with embodiments of the

invention, peer consumer 120 may invoke a smart contract (e.g., smart contract SC2 of the examples above) to discover the IoT data service registered by peer provider 110.

[0027] If peer consumer 120 wishes to consume data of the data service, peer consumer 120 obtains a data service token for the data from blockchain 150 at block 303 of flow 300, as illustrated by arrow 203 of FIGURE 2. For example, peer consumer 120 may analyze information (e.g., data type, valid time, etc.) with respect to the registered data service to determine if data of IoT data 131 is relevant or useful for one or more purpose of the peer consumer. If it is determined that peer consumer 120 desires to consume some portion of IoT data 131, peer consumer 120 may invoke a smart contract (e.g., smart contract SC3 of the examples above) to request a data token for the data service (e.g., data service token comprising a security token, such as a digital signature in the form of "data_access_secret"), according to embodiments of the invention. The data token may, for example, be generated by operation of the aforementioned smart contract (e.g., data_access_secret may be a pseudo random number, such as hash(peer_provider + peer_consumer + cryptopgrapic nonce), where '+' means append, generated when smart contract SC3 is called).

[0028] At block 304 of flow 300, peer consumer 120 requests data of IoT data 131 from IoT data server 130 using the data token, as illustrated by arrow 204 of FIGURE 2. In accordance with embodiments, peer consumer 120 may provide the data token (e.g., data_access_secret) obtained from blockchain 150 to IoT data server 130 with a request for some or all of IoT data 131.

[0029] At block 305 of flow 300, IoT data server 130 verifies the data token using blockchain 150, as illustrated by arrow 205 of FIGURE 2. In accordance with embodiments, IoT data server 130, or peer provider 110 operating in cooperation with IoT data server 130, may invoke a smart contract (e.g., smart contract SC4 of the examples above) to check the validity of the data token (e.g., data_access_secret) provided by peer consumer 120.

[0030] If the data token is determined to be valid, IoT data server 130 provides the requested data of IoT data 131 to peer consumer 120 at block 306 of flow 300, as illustrated by arrow 206 of FIGURE 2. In accordance with embodiments of the invention, IoT data server 130, as may be operating in cooperation with peer provider 110, sends requested data (e.g., data_0, data_1 … data_n) of IoT data 131 to peer consumer 120. Thereafter, peer consumer 120 receives the data at block 307 of flow 300.

[0031] As can be appreciated from the foregoing, operation according to blocks 301-307 cooperate to perform data transfer (exchange of data) from peer provider 110 to peer consumer 120 wherein, although blockchain 150 is used to facilitate the data transfer, the data is exchanged off-chain (i.e., raw IoT data is not directly provided by blockchain 150). Accordingly, widespread discovery of and access to IoT data 131 is provided while issues with respect to long processing times and large blockchain storage space in blockchain 150 are avoided. Although IoT data 131 is provided to peer consumer 120 off-chain, embodiments of hybrid blockchain data exchange platform 100 are nevertheless configured to facilitate verification of the integrity of the data of IoT data 131 exchanged off-chain and/or to ensure the irrefutability of the data exchanged.

[0032] FIGURES 4A and 4B show exemplary flow diagrams setting forth a functional flow for verification of the integrity of data of IoT data 131 provided to peer consumer 120 by hybrid blockchain data exchange platform 100. In particular, the example of FIGURES 4A and 4B use a filtering technique for verifying the integrity of the IoT data exchanged off-chain.

[0033] In providing operation for facilitating verification of the integrity of the IoT data according to flow 400A of FIGURE 4A, at block 401 peer provider 110, or IoT data server 130 operating in cooperation with peer provider 110, generates a data structure representative of IoT data 131, or some portion thereof, to be stored by blockchain 150 for use in verifying the integrity of data. The data structure representative of IoT data 131 may, for example, comprise a Bloom filter or other data structure designed to efficiently (e.g., rapidly and memory-efficiently) indicate whether an element is present in a set. In accordance with embodiments of the invention, peer

provider 110 aggregates a number of data of IoT data 131 (e.g., the data of IoT data 131 provided to peer consumer at block 306 of flow 300), and creates a Bloom filter therefrom (e.g., bloom_filter).

[0034] At block 402 of flow 400A, peer provider 110 stores the data structure representative of IoT data 131 to blockchain 150. In accordance with embodiments, peer provider 110 may invoke a smart contract (e.g., smart contract SC5 of the examples above) to save the data structure representative of IoT data 131 (e.g., bloom_filter, such as may comprise [Hash(data_1), Hash(data_2)….Hash(data_n)]) in the distributed ledger of blockchain 150. IoT data server 130 may also save an identifier (e.g., universally unique identifier (UUID)) of the bloom filter record (e.g., bloom_filter_uuid) for repeated requests. For example, in the case that a peer consumer subsequently requests the same IoT data (e.g., data_1) which has been requested by previously by another peer consumer, the data structure representative of the IoT data (e.g., bloom_filter) and resource identifier (e.g., bloom_filter_uuid) have already saved in the ledger of blockchain 150. Thus, the IoT data server may avoid invoking SC5 to save the bloom value again and may send the resource identifier (e.g., bloom_filter_uuid) and the IoT data (e.g., data_1) directly to the subsequent peer consumer.

[0035] In operation according to embodiments, IoT data server 130 may notify peer consumer 120 (e.g., at block 402 of flow 400A) that the data of IoT 131 may be verified. For example, IoT data server 130 may provide a resource identifier (e.g., bloom_filter_uuid) corresponding to a Bloom filter stored by blockchain 150 to peer consumer 120, whereby peer consumer 120 is apprised of the ability to verify the data by having been provided access to the Bloom filter used for this purpose.

[0036] The operations of blocks 401 and 402 of flow 400A may be performed as part of the operations of flow 300, or separately. For example, operations of blocks 401 and/or 402 may be performed as part of the operations to provide the data at block 306. Operations of blocks 401 and/or 402 may likewise be performed after the operations of flow 300 have been completed (e.g., after completion of the operations of block 307).

[0037] In operation for facilitating verification of the integrity of the IoT data according to flow 400B of FIGURE 4B, at block 411 peer consumer 120 uses the data structure stored by blockchain 150 representative of the data of IoT data to verify the data of IoT data received from IoT data server 130. In accordance with embodiments, peer consumer 120 may invoke a smart contract (e.g., smart contract SC6 of the examples above) with the resource identifier (e.g., bloom_filter_uuid) corresponding to a Bloom filter stored by blockchain 150 to verify data of IoT data 131 obtained from IoT data server 130. For example, if Hash(data_x) is an element of the Bloom filter (e.g., bloom_filter obtained from blockchain 150), the data received by peer consumer 120 from IoT data server 130 may be determined to be valid. Peer consumer 120 and peer provider 110 may, for example, use a predefined hash function (e.g., SHA1) for the hash value computation of the IoT data. IoT data server 130 of embodiments may create a mapping in the ledger (bloom_filter_uuid: bloom_value/bloom_filter), such as through operation of a smart contract (e.g., smart contract SC5, discussed above). Accordingly, peer consumer 120 may receive the resource identifier (e.g., bloom_filter_uuid) and IoT data (e.g., data_1) from the IoT data server and use the predefined hash function (e.g., SHA1) to compute a hash value (e.g., Hash(data_1)). In operation according to embodiments, peer consumer 120 may invoke smart contract SC6 with bloom_filter_uuid and Hash(data_1), whereby blockchain 150 queries the bloom_filter with the bloom_filter_uuid, and tests whether Hash(data_1) is a member of the bloom_filter.

[0038] The operations of block 411 of flow 400B may be performed as part of the operations of flow 300, or separately. For example, operations of block 411 may be performed as part of the operations of peer consumer 120 receiving data from IoT data server 130 at block 307. Operations of block 411 may likewise be performed after the operations of flow 300 have been completed (e.g., after completion of the operations of block 307).

[0039] FIGURES 5A and 5B show exemplary flow diagrams setting forth a functional flow for ensuring the irrefutability of the data exchanged between IoT data server 120 and peer consumer 120 by hybrid blockchain data exchange platform 100. In particular, the example of FIGURES 5A and 5B use a data encryption and key exchange technique for ensuring irrefutability (i.e., peer provider 110 cannot deny on data sent and peer consumer 120 cannot deny on data received) of the IoT data exchanged off-chain.

[0040] In providing operation for ensuring the irrefutability of the data exchanged according to flow 500A of FIGURE 5A, at block 501 data of IoT data 131 requested by peer consumer 120 is encrypted. In accordance with embodiments of the invention, peer provider 110, or IoT data server 130 operating in cooperation with peer provider 110, encrypts the data of IoT data 131 to be sent to peer consumer 120. For example, the data may be encrypted according to the following:

encrypted_data = E(data_0 + data_1 … data_n, key).

[0041] At block 502 of flow 500A, information for use in peer consumer 120 extracting the data is generated. Information used in peer consumer 120 extracting the data may, for example, include a representative data structure, such as a hash value, in addition to a cryptographic key, etc. In accordance with embodiments, peer provider 110, or IoT data server 130 operating in cooperation with peer provider 110, may compute a representative data structure (e.g., hash value) for the data to be used by peer consumer 120 in extracting the data. For example, the representative data structure may be computed according to the following:

hash_value = Hash(encrypted_data).

[0042] At block 503 of flow 500A, information for use in peer consumer 120 extracting the data is stored within blockchain 150 by peer provider 110. In accordance with embodiments of the invention, peer provider 110 may invoke a smart contract (e.g., smart contract SC7 of the examples above) to save the representative data structure (e.g., hash_value) and a cryptographic key corresponding to the encryption of block 501 in the distributed ledger of blockchain 150. It should be appreciated that the encryption may comprise symmetric encryption (e.g., a same cryptographic key is used for encryption and decryption of the data) or asymmetric encryption (e.g., different cryptographic keys, such as public/private keys, are used for encryption and decryption of the data).

[0043] At block 504 of flow 500A, IoT data server 130 provides to peer consumer 120 an instance of encrypted data comprising requested data of IoT data 131, and information for verification of the data received from IoT data server 130. In accordance with embodiments, IoT data server 130, as may be operating in cooperation with peer provider 110, may send encrypted data of IoT data 131 (e.g., encrypted_data generated at block 501 of flow 500A) and a function (e.g., hash function hash_value = Hash(encrypted_data)) from which the representative data structure (e.g., hash_value generated in block 502 of flow 500A) for the encrypted data was generated to peer consumer 120.

[0044] The operations of blocks 501-504 of flow 500A may be performed as part of the operations of flow 300, or separately. For example, operations of blocks 501, 502, 503, and/or 504 may be performed as part of the operations to provide the data at block 306. Operations of blocks 501, 502, 503, and/or 504 may likewise be performed at other times in relation to the operations of flow 300.

[0045] In operation for ensuring the irrefutability of the data exchanged according to flow 500B of FIGURE 5B, at block 511 peer consumer 120 receives encrypted data of IoT data 131 and the information for verification of the data received from IoT data server 130. In accordance with embodiments, peer consumer 120 may receive the encrypted data of IoT data 131 (e.g., encrypted_data) and a function (e.g., the hash function hash_value = Hash(encrypted_data)) from which the representative data structure (e.g., hash_value) for the encrypted data was generated from IoT data server 130.

[0046] At block 512 of flow 500B, the information for verification of the data received from IoT data server 130 is used with the encrypted data of IoT data 131 received from IoT data server 130 to generate information for use in peer consumer 120 extracting the data. In accordance with embodiments, peer consumer 120 may utilize the function (e.g., the hash function hash_value = Hash(encrypted_data)) with the encrypted data of IoT data 131 to compute a representative data structure (e.g., hash_value) for the data.

[0047] At block 513 of flow 500B, the information for verification of the data received from IoT data server 130 is included in a request for a cryptographic key for the encrypted data of IoT data 131. In accordance with embodiments of the invention, peer consumer 120 may invoke a smart contract (e.g., smart contract SC8 of the examples above) to provide the representative data structure (e.g., hash_value) for the data to blockchain 150 for obtaining a cryptographic key used to decrypt the encrypted data of IoT data 131.

[0048] In operation according to embodiments of the invention, blockchain 150 verifies that the representative data structure (e.g., hash_value) stored in the distributed ledger by peer provider 110 and the representative data structure (e.g., hash_value) provided in the request from peer consumer 120 match (i.e., the encrypted data received by peer consumer 120 is the same as the encrypted data generated/provided by peer provider 110 and/or IoT data server 130). Accordingly, peer consumer 120 cannot deny on the data received because no one but one who has received the encrypted data of IoT data 131 (e.g., encrypted_data) can provide the proper representative data structure (e.g., hash_value). Correspondingly, peer provider 110 cannot deny on the data sent because the representative data structure (e.g., hash_value) of the encrypted data has been saved in the distributed ledger of blockchain 150 from processing the request made by peer consumer 120.

[0049] If the encrypted data of IoT data 131 received by peer consumer 120 is verified to be the encrypted data of IoT data 131 generated/provided by peer provider 110 and/or IoT data server 130, blockchain 150 provides the requested cryptographic key for the encrypted data of IoT data 131 to peer consumer 120. Thus, at block 514 of flow 500B, peer consumer 120 receives the requested cryptographic key for the encrypted data of IoT data 131. In accordance with embodiments, the representative data structure (e.g., hash_value) provided in the request from peer consumer 120 is compared to the representative data structure (e.g., hash_value) stored in the distributed ledger by peer provider 110 to determine if they match and, if so, the cryptographic key corresponding to the encryption of block 501 stored in blockchain 150 by peer provider 110 is provided to peer consumer 120.

[0050] At block 515 of flow 500B, data of IoT data 131 is extracted from the encrypted data by peer consumer 120 using the cryptographic key received from blockchain 150. In accordance with embodiments of the invention, peer consumer 120 decrypts the data of IoT data 131 (e.g., data_0, data_1 … data_n) according to the following:

decrypted_data = D(encrypted_data, key).

Thereafter, peer consumer 120 may utilize the data as desired.

[0051] The operations of blocks 511-515 of flow 500B may be performed as part of the operations of flow 300, or separately. For example, operations of blocks 511, 512, 513, 514, and/or 515 may be performed as part of the operations to provide the data at block 307. Operations of blocks 511, 512, 513, 514, and/or 515 may likewise be performed at other times in relation to the operations of flow 300.

[0052] It should be appreciated that, when implemented in software, the functions of flows 300, 400A, 400B, 500A, and 500B providing aspects hybrid blockchain data exchange of the present invention may comprise code segments to perform the tasks as described herein. The code segments can be stored in a processor readable medium for execution by one or more processors of a processor-based system. The processor readable medium may include any medium that can suitably store and transfer information. Examples of the processor readable medium include an

electronic circuit, a semiconductor memory device, a read only memory (ROM), a flash memory, an erasable ROM (EROM), an optical disk, a hard disk, etc. The code segments may be downloaded via computer networks such as a local area network (LAN), a wide area network (WAN), the Internet, an intranet, a cellular communication network, etc.

[0053] As can be appreciated from the foregoing exemplary embodiments, concepts of the present invention provide for data exchange using a distributed ledger, wherein data is exchanged off-chain and information for accessing the off-chain data is exchanged through the blockchain. Accordingly, hybrid blockchain implementations avoid storing the bulk of the data within the blockchain and provide solutions well suited for data exchange with respect to very large volumes of data, such as IoT data. It should be appreciated, however, that the concepts herein are not limited to use with respect to exchange of IoT data. For example, embodiments of a hybrid blockchain data exchange platform may be utilized with respect to various large databases, such as banking or merchant transaction records, video on demand libraries, public or governmental data sharing (e.g., map data, statistical data, etc.), document or music file sharing, etc.

[0054] Although the present invention and its advantages have been described in detail, it should be understood that various changes, substitutions and alterations can be made herein without departing from the spirit and scope of the invention as defined by the appended claims. Moreover, the scope of the present application is not intended to be limited to the particular embodiments of the process, machine, manufacture, composition of matter, means, methods and steps described in the specification. As one of ordinary skill in the art will readily appreciate from the disclosure of the present invention, processes, machines, manufacture, compositions of matter, means, methods, or steps, presently existing or later to be developed that perform substantially the same function or achieve substantially the same result as the corresponding embodiments described herein may be utilized according to the present invention. Accordingly, the appended claims are intended to include within their scope such processes, machines, manufacture, compositions of matter, means, methods, or steps.

CLAIMS

What is claimed is:

1. A method for exchange of data from a peer provider to a peer consumer, the method comprising:

storing, by a data server for the peer provider, data available for exchange with one or more peer consumers;

registering, by the peer provider using a blockchain network, a data service for the data available for exchange;

receiving, by the data server or the peer provider from the peer consumer, a request for data of the data available for exchange, wherein the request for data includes a data token of the data service for the data available for exchange obtained by the peer consumer from the blockchain network;

verifying, by the data sever or the peer provider using the blockchain network, the data token; and

providing, by the data server to the peer consumer, requested data of the data available for exchange if the verifying the data token confirms validity of the data token.

2. The method of claim 1, wherein the registering the data service comprises:

invoking a first smart contract of the blockchain network to register the data service.

3. The method of claim 2, wherein the data token is obtained by the peer consumer after the peer consumer invokes a second smart contract of the blockchain network to discover the data service registered by peer provider, and after the peer consumer invokes a third smart contract of the blockchain network to request the data token.

4. The method of claim 2, wherein the verifying the data token comprises:

invoking a fourth smart contract of the blockchain network to check the validity of the data token provided by the peer consumer.

5. The method of claim 1, wherein the data available for exchange comprises Internet of Things (IoT) data.

6. The method of claim 1, wherein the data token is a security token comprising a digital signature.

7. The method of claim 1, wherein the blockchain network is a permissioned private blockchain network.

8. The method of claim 1, wherein the blockchain network does not include the data server and does not store the data available for exchange, and wherein the providing the requested data by the data server to the peer consumer exchanges the requested data by the data server to the peer consumer off-chain with respect to the blockchain network.

9. The method of claim 1, further comprising:

generating, by the data server or the peer provider, a data structure representative of the data available for exchange; and

storing the data structure representative of the data available for exchange to the blockchain network.

10. The method of claim 9, wherein the storing the data structure to the blockchain comprises:

invoking a fifth smart contract of the blockchain network to save the data structure representative of the data available for exchange in the distributed ledger of the blockchain network.

11. The method of claim 9, wherein the data structure representative of the data available for exchange to the blockchain network comprises a Bloom filter for the data available for exchange to the blockchain network.

12. The method of claim 9, wherein the data structure representative of the data available for exchange is made available to the peer consumer by the blockchain network as part of the data service for verifying integrity of the requested data.

13. The method of claim 12, wherein the data structure representative of the data available for exchange is obtained by the peer consumer after the peer consumer invokes a sixth smart contract of the blockchain network as part of operation to verify data of the data available for exchanged obtained from data server by the peer consumer.

14. The method of claim 1, further comprising:

encrypting the requested data, wherein the providing the requested data comprises providing an encrypted instance of the requested data to the peer consumer by the data server;

generating information for use in the peer consumer extracting the requested data from the encrypted instance of the requested data; and

storing the information for use in the peer consumer extracting the requested data and a cryptographic key for the encrypted instance of the requested data to the blockchain network.

15. The method of claim 14, wherein the storing the information for use in the peer consumer extracting the requested data and the cryptographic key to the blockchain network comprises:

invoking a seventh smart contract of the blockchain network to save the information for use in the peer consumer extracting the requested data and the cryptographic key in a distributed ledger of the blockchain network.

16. The method of claim 14, wherein the providing the encrypted instance of the requested data to the peer consumer by the data server also provides information for verification of data received from the data server, wherein the cryptographic key is obtained by the peer consumer after the peer consumer generates, using the encrypted instance of the requested data and the information for verification of data received from the data server, corresponding information for use in the peer consumer extracting the requested data and invokes an eighth smart contract of the blockchain network to provide the corresponding information for use in the peer consumer extracting the requested data to the blockchain network.

17. The method of claim 16, wherein the information for use in the peer consumer extracting the requested data comprises a hash value for the encrypted instance of the requested data, and wherein the information for verification of data received from the data server comprises a hash function used to generate the hash value.

18. A hybrid blockchain data exchange system comprising:

a data server storing data available for exchange with one or more peer consumers;

a peer provider system configured to register a data service for the data available for exchange using a blockchain network, wherein the hybrid blockchain data exchange system is configured to receive a request from a peer consumer system for data of the data available for exchange stored by the data server, wherein the request for data includes a data token of the data service, wherein the hybrid blockchain data exchange system is configured to use the blockchain network to verify the data token and provide to the peer consumer system requested data of the data available for exchange if the data token is verified.

19. The hybrid blockchain data exchange system of claim 18, wherein the data available for exchange comprises Internet of Things (IoT) data.

20. The hybrid blockchain data exchange system of claim 18, wherein the blockchain network is a permissioned private blockchain network.

21. The hybrid blockchain data exchange system of claim 18, wherein the blockchain network does not include the data server and does not store the data available for exchange, and wherein the hybrid blockchain data exchange system is configured to provide the requested data to the peer consumer off-chain with respect to the blockchain network.

22. The hybrid blockchain data exchange system of claim 18, wherein the hybrid blockchain data exchange system is configured to generate a data structure representative of the data available for exchange and to store the data structure representative of the data available for exchange to the blockchain network, and wherein the data structure representative of the data available for exchange is made available to the peer consumer by the blockchain as part of the data service for verifying integrity of the requested data.

23. The hybrid blockchain data exchange system of claim 18, wherein the hybrid blockchain data exchange system is configured to encrypt encrypting the requested data as provided to the peer consumer by the data server, to generate generating information for use in the peer consumer extracting the requested data from an encrypted instance of the requested data, and to store storing the information for use in the peer consumer extracting the requested data and a cryptographic key for the encrypted instance of the requested data to the blockchain network, wherein the cryptographic key is obtained by the peer consumer after the peer consumer generates, using the encrypted instance of the requested data and the information for verification of data received from the data server, corresponding information for use in the peer consumer extracting the requested data.

24. A method for exchange of data by a hybrid blockchain data exchange system from a peer provider to a peer consumer, the method comprising:

storing, by a data server for the peer provider, data available for exchange with one or more peer consumers;

invoking a first smart contract of a blockchain network by the peer provider to register a data service for the data available for exchange, wherein a data token is obtained by the peer consumer after the peer consumer invokes a second smart contract of the blockchain network to discover the data service registered by peer provider, and after the peer consumer invokes a third smart contract of the blockchain network to request the data token;

receiving a request from the peer consumer for data of the data available for exchange, wherein the request for data includes the data token of the data service for the data available for exchange obtained by the peer consumer from the blockchain network;

invoking a fourth smart contract of the blockchain network to check the validity of the data token provided by the peer consumer; and

providing, by the data server to the peer consumer, requested data of the data available for exchange if the verifying the data token confirms validity of the data token.

25. The method of claim 24, further comprising:

generating, by the data server or the peer provider, a data structure representative of the data available for exchange; and

invoking a fifth smart contract to save the data structure representative of the data available for exchange to the blockchain network, wherein the data structure representative of the data available for exchange is made available to the peer consumer by the blockchain network as part of the data service for verifying integrity of the requested data, and wherein the data structure representative of the data available for exchange is provided to the peer consumer after the peer consumer invokes a sixth smart contract of the blockchain network as part of operation to verify data of the data available for exchanged obtained from data server by the peer consumer.

26. The method of claim 24, further comprising:

encrypting the requested data, wherein the providing the requested data comprises providing an encrypted instance of the requested data to the peer consumer by the data server;

generating information for use in the peer consumer extracting the requested data from the encrypted instance of the requested data; and

invoking a seventh smart contract of the blockchain network to save the information for use in the peer consumer extracting the requested data and a cryptographic key for the encrypted instance of the requested data to the blockchain network, wherein the information for verification of data received from the data server is provided to the peer consumer by the data server with the

encrypted instance of the requested data, wherein the cryptographic key is provided to the peer consumer after the peer consumer generates, using the encrypted instance of the requested data and the information for verification of data received from the data server, corresponding information for use in the peer consumer extracting the requested data and invokes an eighth smart contract of the blockchain network to provide the corresponding information for use in the peer consumer extracting the requested data to the blockchain network.

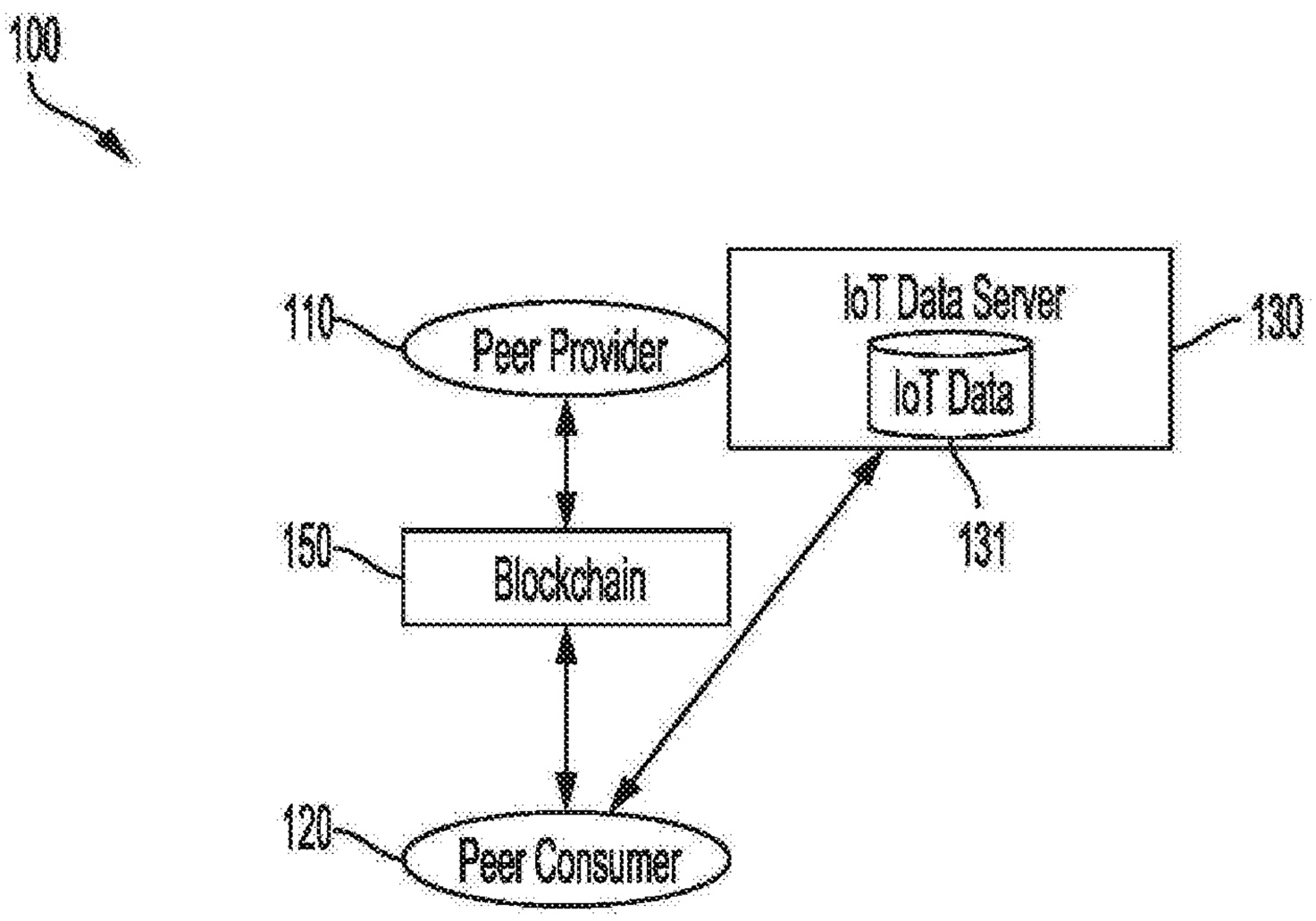
100
110
Peer Provider
IoT Data Server
IoT Data
130
131
150
Blockchain
120
Peer Consumer

FIG. 1

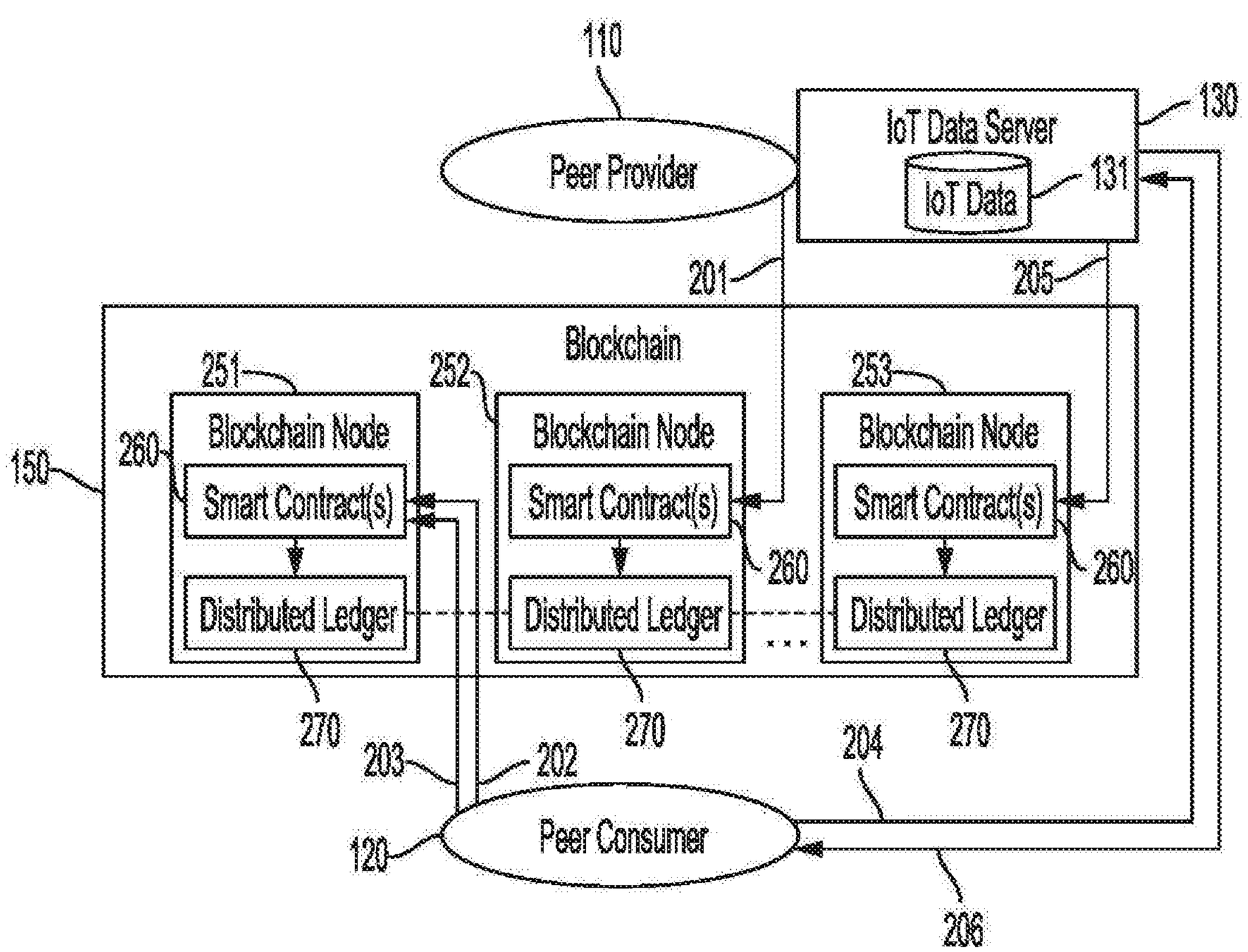
110
Peer Provider
IoT Data Server
IoT Data
130
131
201
205
Blockchain
251
252
253
Blockchain Node
Blockchain Node
Blockchain Node
260
150
Smart Contract(s)
Smart Contract(s)
Smart Contract(s)
260
260
Distributed Ledger
Distributed Ledger
Distributed Ledger
270
270
270
203
202
204
120
Peer Consumer
206

FIG. 2

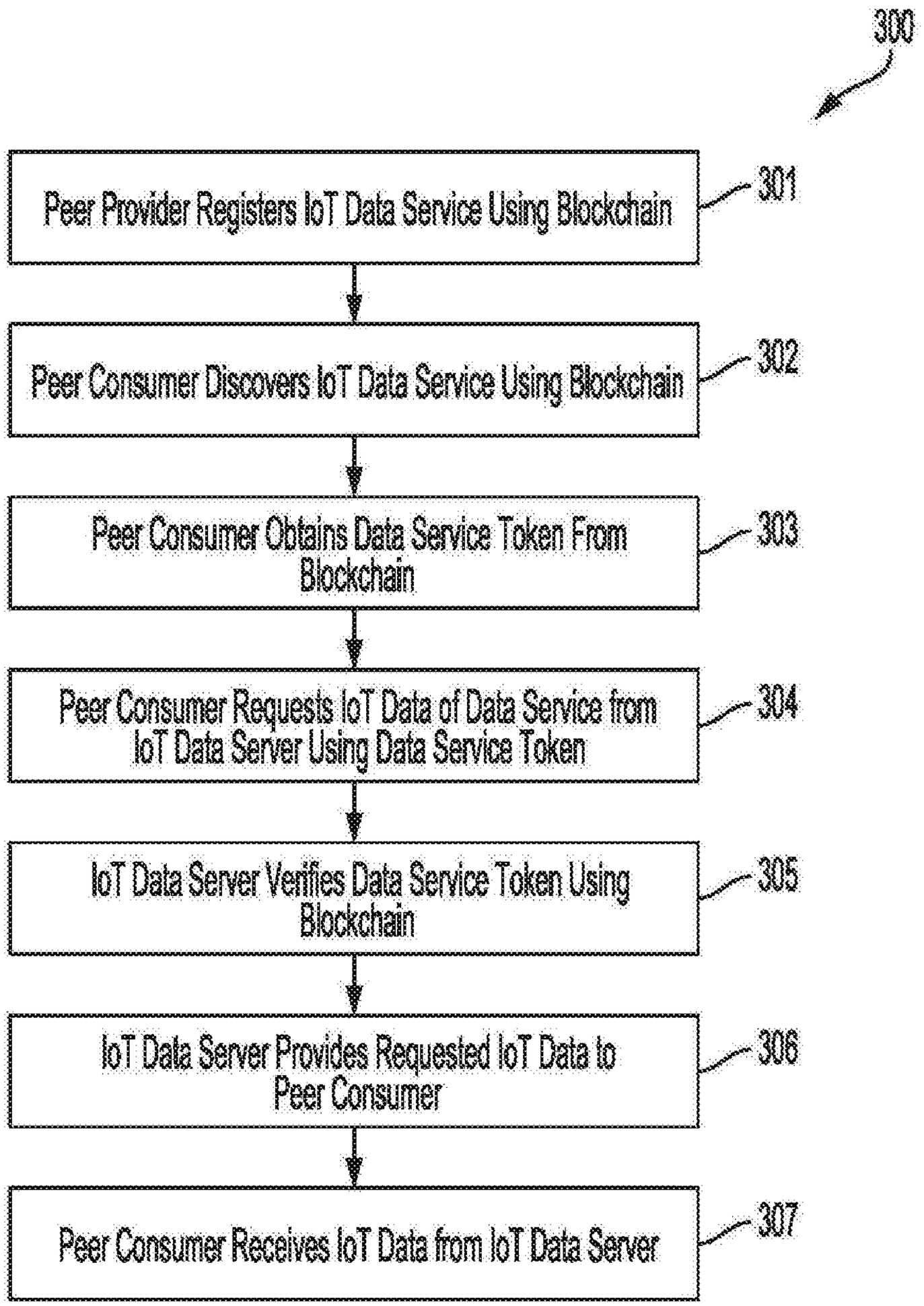
300
Peer Provider Registers IoT Data Service Using Blockchain
301
Peer Consumer Discovers IoT Data Service Using Blockchain
302
Peer Consumer Obtains Data Service Token From Blockchain
303
Peer Consumer Requests IoT Data of Data Service from IoT Data Server Using Data Service Token
304
IoT Data Server Verifies Data Service Token Using Blockchain
305
IoT Data Server Provides Requested IoT Data to Peer Consumer
306
Peer Consumer Receives IoT Data from IoT Data Server
307

FIG. 3

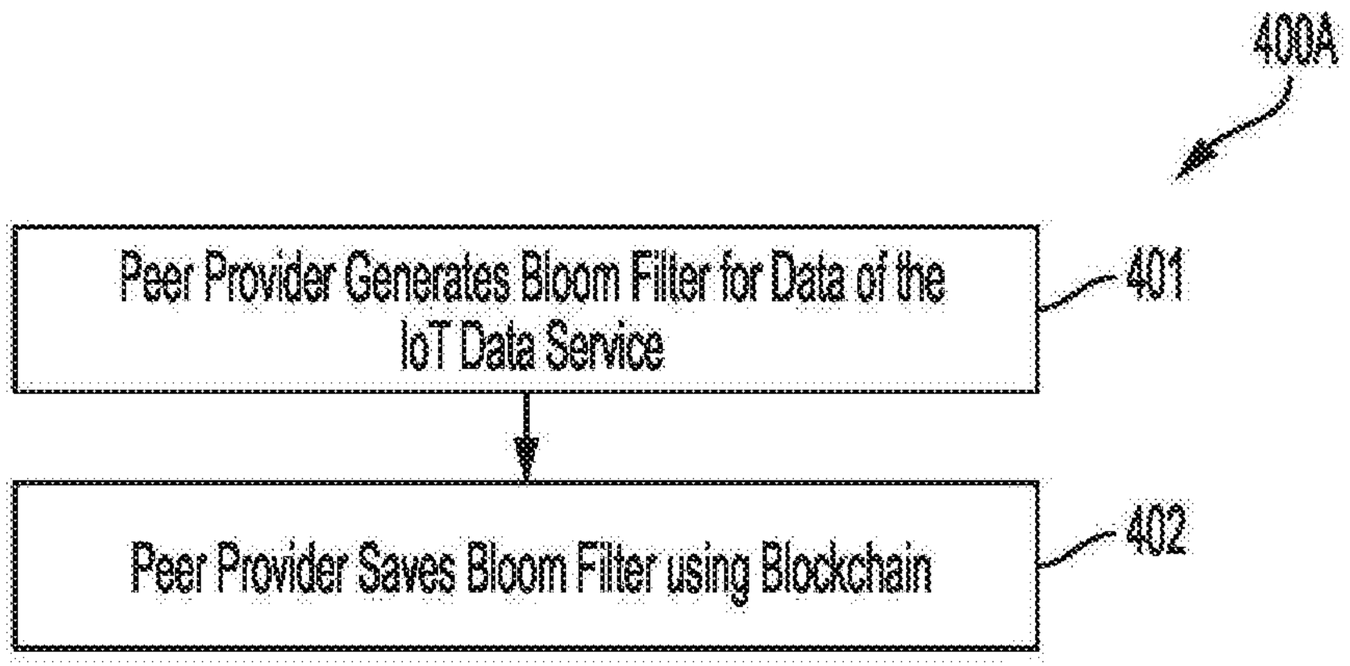
400A
Peer Provider Generates Bloom Filter for Data of the IoT Data Service
401
Peer Provider Saves Bloom Filter using Blockchain
402

FIG. 4A

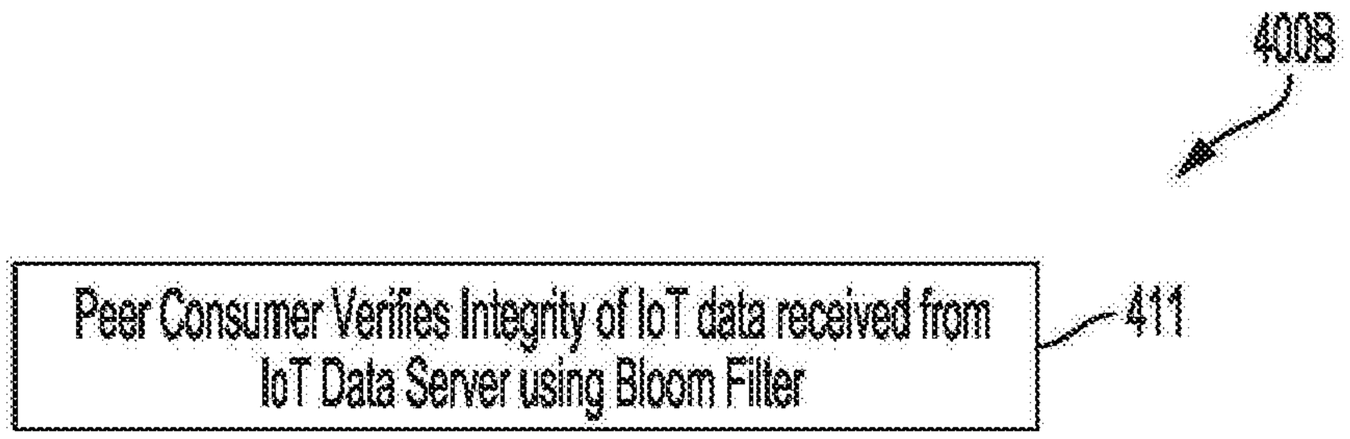
400B
Peer Consumer Verifies Integrity of IoT data received from IoT Data Server using Bloom Filter
411

FIG. 4B

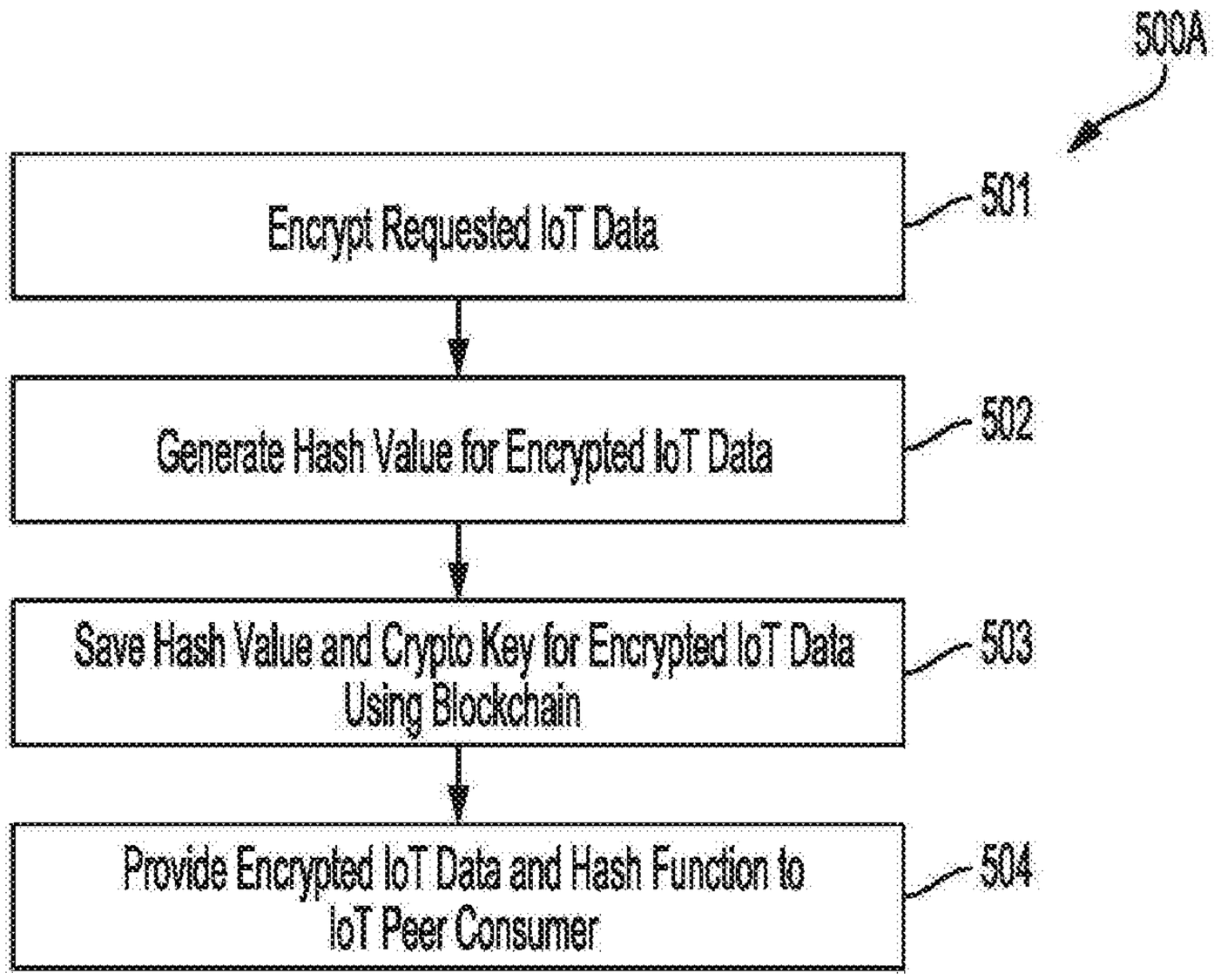
500A
Encrypt Requested IoT Data
501
Generate Hash Value for Encrypted IoT Data
502
Save Hash Value and Crypto Key for Encrypted IoT Data Using Blockchain
503
Provide Encrypted IoT Data and Hash Function to IoT Peer Consumer
504

FIG. 5A

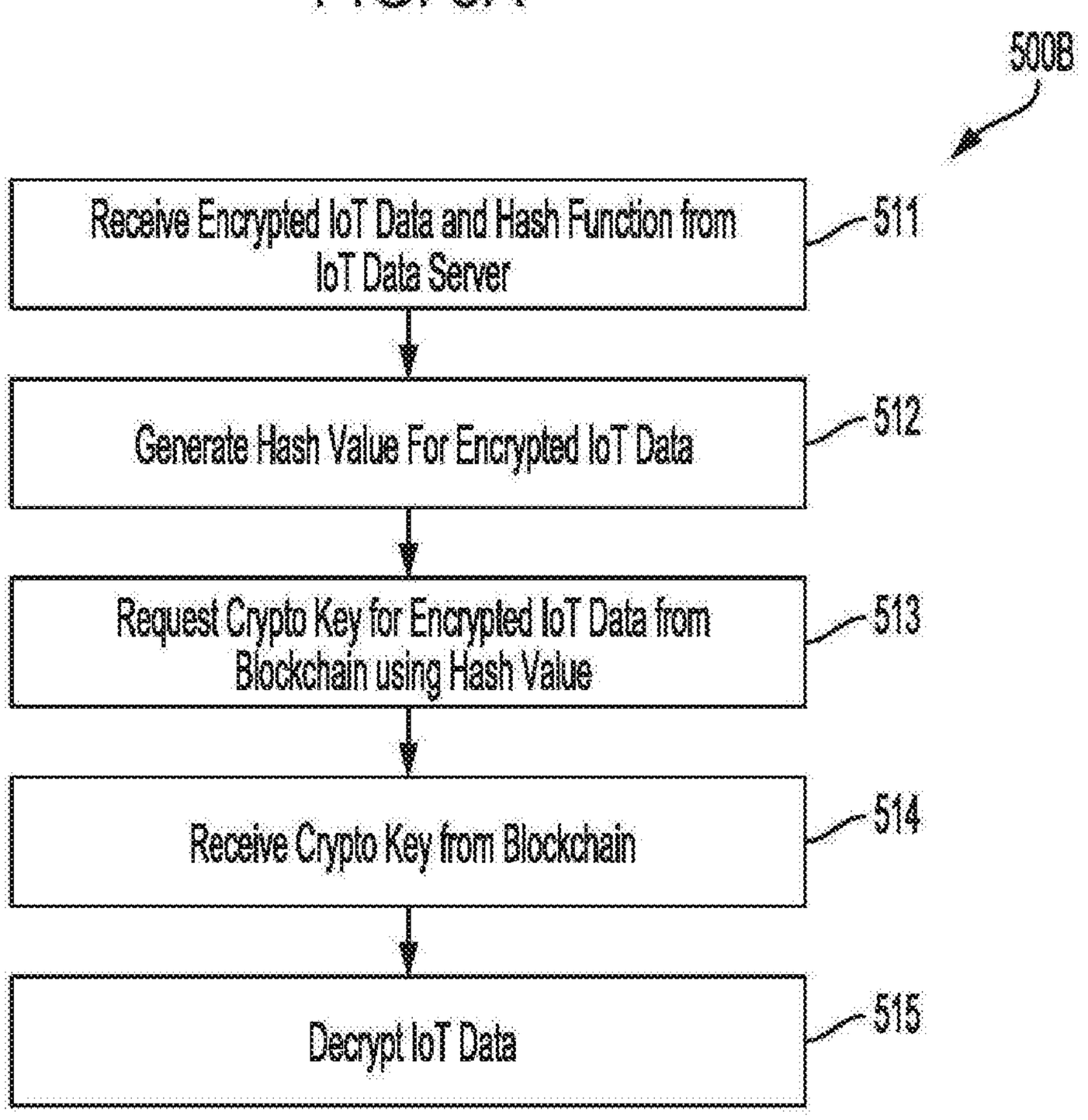
500B
Receive Encrypted IoT Data and Hash Function from IoT Data Server
511
Generate Hash Value For Encrypted IoT Data
512
Request Crypto Key for Encrypted IoT Data from Blockchain using Hash Value
513
Receive Crypto Key from Blockchain
514
Decrypt IoT Data
515

FIG. 5B

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/071953

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(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

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

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

CNPAT,CNKI,WPI,EPODOC: blockchain, peer, provider, consumer, data, token, discover, verify, exchange, smart, contract, encrypt

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 108156232 A (YIJIE, Wang) 12 June 2018 (2018-06-12) description paragraphs [0019]-[0054], claims 1-10	1-26
Y	CN 109450910 A (YUANGUANG SOFTWARE CO., LTD.) 08 March 2019 (2019-03-08) description paragraphs [0059]-[0138], claims 1-10	1-26
A	CN 109450849 A (JIANNAN, Tang) 08 March 2019 (2019-03-08) the whole document	1-26
A	CN 110189121 A (ALIBABA GROUP HOLDING LIMITED) 30 August 2019 (2019-08-30) the whole document	1-26
A	US 2019342290 A1 (MASTERCARD INTERNATIONAL INCORPORATED) 07 November 2019 (2019-11-07) the whole document	1-26

☐ 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	Date of mailing of the international search report
17 September 2020	**29 September 2020**
Name and mailing address of the ISA/CN **National Intellectual Property Administration, PRC** **6, Xitucheng Rd., Jimen Bridge, Haidian District, Beijing** **100088** **China** Facsimile No. **(86-10)62019451**	Authorized officer **WANG,Lunjie** Telephone No. **(86-10)53961776**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2020/071953

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	108156232	A	12 June 2018	None			
CN	109450910	A	08 March 2019	None			
CN	109450849	A	08 March 2019	None			
CN	110189121	A	30 August 2019	None			
US	2019342290	A1	07 November 2019	WO	2019212663	A1	07 November 2019
				CN	110445612	A	12 November 2019