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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 November 2022 (24.11.2022)

WIPO | PCT

(10) International Publication Number
WO 2022/245663 A1

(51) International Patent Classification:
G06Q 30/00 (2012.01)

(21) International Application Number:
PCT/US2022/029242

(22) International Filing Date:
13 May 2022 (13.05.2022)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
63/189,822 18 May 2021 (18.05.2021) US

(71) Applicant: **COVESTRO LLC** [US/US]; 1 Covestro Circle, Pittsburgh, Pennsylvania 15205 (US).

(72) Inventors: **OWENS, Steven G.**; 251 Ritter Road, Sewickley, Pennsylvania 15143 (US). **STEPPAN, David D.**; 104 Drury Court, Gibsonia, Pennsylvania 15044 (US). **PHELAN, Gerald W.**; 115 Fawn Valley Drive, McMurray, Pennsylvania 15317 (US). **CLOHERTY, Scott M.**; 738 Mission Hills Drive, Canonsburg, Pennsylvania 15317 (US). **ULAM, Devin W.**; 526 North Meadowcroft Avenue, Pittsburgh, Pennsylvania 15216 (US).

(74) Agent: **BENDER, Richard P.**; 1 Covestro Circle, Pittsburgh, Pennsylvania 15205 (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, IQ, IR, IS, IT, JM, 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, ST, SV, SY, TH, TJ, TM,

(54) Title: BLOCKCHAIN VERIFICATION SYSTEM FOR GREEN RATING SYSTEM AND BUILDING CODE COMPLIANCE

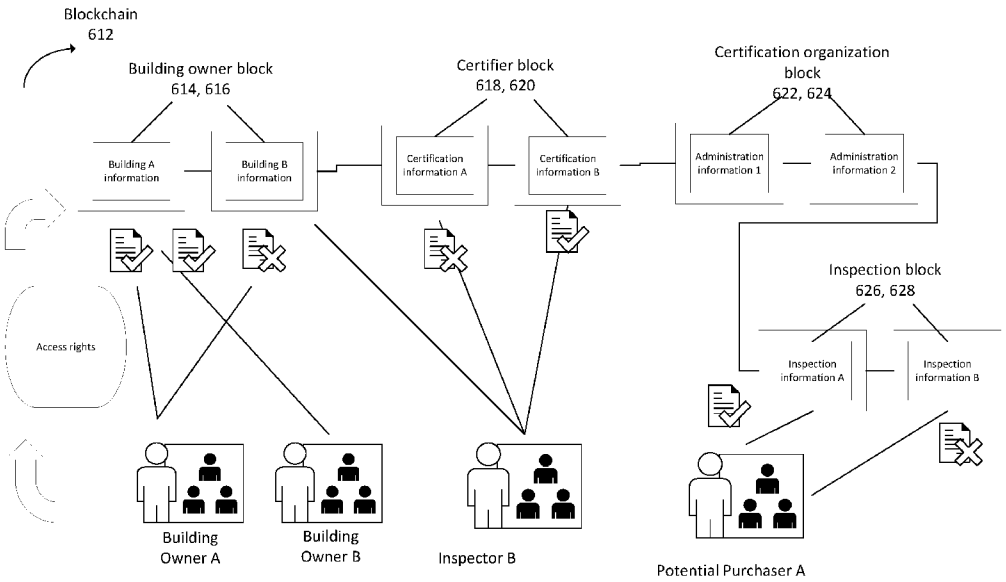

FIG. 6B

(57) Abstract: A method of securing data associated with one or more building rating systems includes identifying information relevant to one or more building rating systems for a target building, including, without limitation, information about the target building, inspection information pertaining to the target building, and information pertaining to the one or more building rating systems, and storing at least a portion of this information to a blockchain. At least a portion of the blockchain is accessible by one or more building owners, certifiers, inspectors, certification organizations, and/or potential purchasers according to an access policy associated with the blockchain, where the access policy includes an access control list that defines one or more access rights to the blockchain.

WO 2022/245663 A1

[Continued on next page]

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))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

TITLE - BLOCKCHAIN VERIFICATION SYSTEM FOR GREEN RATING SYSTEM AND BUILDING CODE COMPLIANCE

BACKGROUND

[0001] Assessing compliance of a building or construction project with the applicable building codes and/or certification or rating systems such as, for example, with fire-resistance rating system requirements, green building rating systems (e.g., Leadership in Energy and Environmental Design (LEED)), and/or the like, typically involves contributing and tracking a significant amount of information across the design, material and system specifications, construction, and use of the project.

[0001] Initially, this information is compiled by the designer and submitted to appropriate officials or third party verifiers for pre-construction compliance approval. As the project moves into the construction phase, a vast array of building materials and building and construction equipment are ordered as well as multiple trades are scheduled. Invariably, order and construction sequence changes occur that must be appropriately documented. Officials and other inspectors/verifiers responsible for assurance of compliance with the codes and/or certification or rating systems must independently verify that the as-built information equally fulfills compliance.

[0002] This document describes methods and systems that are directed to addressing the problems, challenges and complexities described above, and/or other issues.

SUMMARY

[0003] This disclosure is not limited to the particular systems, methodologies or protocols described, as these may vary. The terminology used in this description is for the purpose of describing the particular versions or embodiments, and is not intended to limit the scope.

[0004] As used in this document, the singular forms "a," "an," and "the" include plural references unless the context clearly dictates otherwise. Unless defined otherwise, all technical and scientific terms used in this document have the same meanings as commonly understood by one of ordinary skill in the art. As used in this document, the term "comprising" means "including, but not limited to."

[0005] In an embodiment, a method of securing data associated with one or more building rating systems includes, by one or more electronic devices, receiving, from a building owner of a target building that is a subject of a building rating system, a communication that includes building information corresponding to the target building, generating a building owner block that is associated with the building owner, storing at least a portion of the building information in the building owner blocks, adding the building owner block to a blockchain, identifying a certifier associated with the target building, and receiving, from the identified certifier, a communication that includes certification information corresponding to the target building. The certification information includes at least a portion of the building information that the certifier has retrieved from the building owner block. The method includes generating a certifier block that is associated with the identified certifier, storing at least a portion of the certification information in the certifier block, adding the certifier block to the blockchain,

identifying an inspector associated with a certification organization responsible for administering the building rating system, and receiving, from the identified inspector, a communication comprising inspection information corresponding to the target building. The inspection information includes information pertaining to compliance of the target building or one or more components of the target building with one or more requirements of the building rating system. The method includes generating an inspection block that is associated with the identified inspector, storing at least a portion of the inspection information in the inspection block, and adding the inspection block to the blockchain. At least a portion of the blockchain is accessible by the building owner, the certifier, the certification organization, and/or one the inspector according to an access policy associated with the blockchain. The access policy includes an access control list that defines one or more access rights to the blockchain.

[0006] In various embodiments, a computer program that includes one or more programming instructions, that when executed by one or more electronic devices, causes the one or more electronic devices to perform the above-described method is disclosed.

[0007] In various embodiments, a system for securing data associated with one or more building rating systems includes one or more electronic devices and a computer-readable storage medium is disclosed. The computer-readable storage medium includes one or more programming instructions that, when executed, cause one or more of the one or more electronic devices to perform the above-described method.

[0008] In various embodiments, a non-transitory computer-readable storage medium includes one or more programming instructions that, when executed by one or more processors, performs the above-described method.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] FIG. 1 illustrates an example building rating system lifecycle.

[0010] FIG. 2 illustrates an example building rating system management system.

[0011] FIG. 3 illustrates an example blockchain structure.

[0012] FIG. 4 illustrates a flow chart of an example method of performing tamper-evident logging.

[0013] FIG. 5 illustrates an example of a source log.

[0014] FIG. 6A illustrates a flow chart of an example method of verifying access requests to a target blockchain.

[0015] FIG. 6B illustrates example access requests according to various embodiments.

[0016] FIG. 7 illustrates an example delegation process.

[0017] FIG. 8 illustrates an example multiple-tier delegation process according to an embodiment.

[0018] FIGS. 9A and 9B illustrate example tokens and data according to various embodiments.

[0019] FIG. 10 illustrates a block diagram of example hardware that may be used to contain or implement program instructions.

DETAILED DESCRIPTION

[0020] The following terms shall have, for purposes of this application, the respective meanings set forth below:

[0021] A "block" or a "node" refers to a data structure that includes a link to one or more other data structures. In certain embodiments, a block may include a grouping of data or data records. A block of a blockchain may include a link to an immediately preceding block in the blockchain, a subsequent block in the blockchain, a different block in the blockchain, or a different block in another blockchain.

[0022] A "blockchain" refers to a distributed data structure that includes a sequence of blocks that are linked together.

[0023] An "electronic device" or a "computing device" refers to a device that includes a processor and memory. Each device may have its own processor and/or memory, or the processor and/or memory may be shared with other devices as in a virtual machine or container arrangement. The memory may contain or receive programming instructions that, when executed by the processor, cause the electronic device to perform one or more operations according to the programming instructions. Examples of electronic devices include personal computers, servers, mainframes, virtual machines, containers, gaming systems, televisions, and mobile electronic devices such as smartphones, personal digital assistants, cameras, tablet computers, laptop computers, media players and the like. In a client-server arrangement, the client device and the server are each electronic devices, in which the server contains instructions and/or data that the client device accesses via one or more communications links in one or more communications networks. In a virtual machine arrangement, a server may be an electronic device, and each virtual machine or container may also be considered to be an electronic device. In the discussion below, a client device, server device, virtual machine or container may be referred to simply as a "device" for brevity.

[0024] The terms "memory," "memory device," "computer-readable storage medium", "data store," "data storage facility" and the like each refer to a non-transitory device on which computer-readable data, programming instructions or both are stored. Except where specifically stated otherwise, the terms "memory," "memory device," "computer-readable storage medium", "data store," "data storage facility" and the like are intended to include single device embodiments, embodiments in which multiple memory devices together or collectively store a set of data or instructions, as well as individual sectors within such devices.

[0025] The terms "processor" and "processing device" refer to a hardware component of an electronic device that is configured to execute programming instructions. Except where specifically stated otherwise, the singular term "processor" or "processing device" is intended to include both single-processing device embodiments and embodiments in which multiple processing devices together or collectively perform a process.

[0026] A "private key" refers to an asymmetric cryptographic key that is used to encrypt or decrypt messages, data, information, or other content. Messages encrypted using a private key may be decrypted by a recipient who possesses an associated public key. Likewise, messages that are encrypted using an associated public key may be decrypted using a private key.

[0027] A "public key" refers to an asymmetric cryptographic key that are generally obtained and used without restriction to encrypt and/or decrypt messages. Messages encrypted using a public key may be decrypted by a recipient who possesses an associated private key. Likewise, messages that are encrypted using a private key may be decrypted by a recipient who possesses an associated public key.

[0028] A "building rating system" refers to one or more requirements, criteria or other forms of assessment pertaining to the performance, compliance, or operation of a building, a

construction project or development, and/or a component or portion thereof. Green building rating systems, which rate relative levels of compliance or performance of a building, development, or portion thereof to one or more specific environmental requirements or goals is an example of a building rating system. A building code compliance system is also an example of a building rating system as the term is used in this document, including fire resistance, water resistance, earthquake resistance, and/or the like. A building rating system may include information that is voluntary, such as, for example, a green building rating system. A building rating system may include information that is mandatory, such as, for example, in building code compliance. The blanket term "building rating system" includes information for systems that apply to the building, that may be useful to different parties or participants as described in this document. Building rating systems may be used to assess new construction or renovations of existing structures.

[0029] There are various types of building rating systems that pertain to buildings, developments, or portions thereof. Green building rating systems are an example of a building rating system. Green building rating systems may rate relative levels of compliance or performance of a building, development, or portion thereof to one or more specific environmental requirements or goals. These environmental requirements or goals may include, for example, metrics or thresholds pertaining to energy savings, water efficiency, emissions reduction, and indoor environmental quality, among others. Leadership in Energy and Environmental Design (LEED) is an example of a green building rating system. LEED provides a point system to score green building design and construction across five basic areas: Sustainable Sites, Water Efficiency, Energy and Atmosphere, Materials and Resources, and Indoor Environmental Quality. Buildings are awarded points based on their compliance with

criteria in these categories, such that the more points that are awarded results in an higher level of certification for the building. LEED awards certifications at the Certified, Silver, Gold, and Platinum levels.

[0030] WELL Certification, Green Globes, Building Research Establishment Environmental Assessment Method (BREEM), and DGNB, are examples of other green building rating systems. It is understood that this disclosure contemplates additional and/or alternate green building rating systems, whether now known or existing in the future.

[0031] Another type of building rating system is a fire-resistance rating system. A fire-resistance rating system may rate the fire risk of one or more assemblies or components of a building (e.g., walls, ceilings, floors, and other building systems) or may determine compliance of one or more of these assemblies or components to code requirements pertaining to fire resistance.

[0032] For example, an assembly may be installed in a temperature-controlled furnace with the temperature increased over a certain period of time in accordance with one or criteria, standards, or requirements of the applicable fire-resistance rating system. If the assembly survives or withstands the fire test for the time period, the assembly is recognized as meeting the applicable rating.

[0033] FIG. 1 illustrates an example building rating system lifecycle for an example building according to various embodiments. An example lifecycle may involve a building owner **102**, a certifier **104**, a certification organization **106**, one or more inspectors **108** and/or one or more potential purchasers **110**.

[0034] A building owner **102** may be one or more individuals, entities and/or organizations who own a building that is the subject of one or more building rating system

reviews. For the purposes of this disclosure, a building or component thereof that is the subject of one or more building rating system reviews is referred to as a "target building." In some embodiments, a building owner **102** may also include one or more individuals, entities and/or organizations that manage, operate, or otherwise run a target building on behalf of the building owner. Examples may include, without limitation, a building or property manager, an operations manager, an architect, and/or the like.

[0035] A building owner **102** may provide building information pertaining to one or more target buildings to a blockchain system, as described in more detail below. Building information may include, without limitation, information about materials used in the construction of at least a portion of a target building, assemblies of the target building, design of the target building and/or the like. Example building information may include, without limitation, identification of the types of materials used, unique identifiers associated with one or more materials used (e.g., model or serial numbers), a supplier of one or more materials or assemblies, a manufacturer of one or more materials or assemblies, an installer of one or more materials and/or assemblies, specifications associated with one or more materials and/or assemblies (e.g., a color, a finish, etc.), and/or the like

[0036] A certifier **104** refers to an individual, entity and/or organization who is responsible for gathering certification information for consideration by a certifying organization with respect to a target building's compliance with one or more building rating systems. Certification information may include, without limitation, information about materials used in the construction of at least a portion of a target building, assemblies of the target building, design of the target building and/or the like. Example certification information may include, without limitation, data pertaining to the target building's energy consumption, energy sources, water

consumption, water sources, location, waste reduction, reuse and recycling, and/or the like. In various embodiments, certification information may include a subset or portion of building information.

[0037] In various embodiments, a certifier **104** may work with a building owner **102** to collect or access relevant certification information for rating/certification consideration. The certifier **104** may provide at least a portion of this certification information to a blockchain system, as described in more detail below. The information that is provided by a certifier (e.g., certification information), may be uniquely correlated with one or more target buildings, for example, by a unique identifier.

[0038] A certification organization **106** refers to an organization or entity that administers one or more building rating systems. This administration may include performing third-party technical reviews and verification of registered projects. As an example, The Green Business Certification Inc. administers LEED. In various embodiments, a certification organization may provide administration information to a blockchain system, as described in more detail below. Administration information may include information pertaining to one or more building rating systems such as, for example, one or more tests to be performed as party of a building rating system, criteria associated with a building rating system, information about the available ratings or certifications for a building rating system, and/or the like. The information that is provided by a certification organization (e.g., administration information), may be uniquely correlated with one or more target buildings, for example, by a unique identifier.

[0039] In various embodiments, one or more inspectors **108** may act on behalf of a certification organization **106**. For instance, a certification organization **106** may employ one or more inspectors **108** to perform reviews of target buildings to determine or verify their

compliance with the applicable building rating systems. In these situations, the inspectors **108** may be affiliated with one or more certification organizations **106**.

[0040] As an example, an inspector **108** may inspect a target building or portions of a target building to determine whether certification information that was provided is accurate and whether the target building is compliant with the applicable building rating system. As another example, an inspector **108** may perform one or more tests or analyses to ascertain whether a target building satisfies one or more building rating systems. For instance, with respect to a fire-resistance rating system, an inspector may conduct one or more tests of one or more assemblies of a target building. For example, an inspector **108** may conduct the fire resistance test ASTM E119-20 (Standard Test Method for Fire Tests of Building Construction and Materials) in the United States. Additional and/or alternate fire-resistance tests and/or rating systems may be used within the scope of this disclosure.

[0041] One or more inspectors **108** may provide inspection information pertaining to one or more inspections of a target building to a blockchain system, as described in more detail below. Inspection information may include information pertaining to compliance of a target building or one or more components of the target building with one or more requirements of a building rating system. For instance, inspection information may include information such as, for example, inspection specifications, an inspection location, a date of inspection, a name of one or more individuals who inspected the target building, one or more images of the inspected target building or portion thereof, results of one or more inspections or tests performed by an inspector, a report or other proof of inspector approval or comments, and/or the like. An image capture device such as, for example, a camera, a video recorder, an infrared imaging device, and/or the like may be used to capture one or more images or videos within the scope of this disclosure.

The information that is provided by an inspector (e.g., inspection information), may be uniquely correlated with one or more target buildings, for example, by a unique identifier.

[0042] In various embodiments, one or more potential purchasers **110** may be involved in the lifecycle of a target building. A potential purchaser **110** may be an individual, entity or organization that is considering acquiring ownership rights and/or usage or access rights to a target building. As part of the diligence process in deciding whether to purchase an interest in a target building, a potential purchaser **110** may wish to access information stored by a blockchain system pertaining to building rating system certifications held by the target building, and/or building rating system tests, reviews, inspections and/or the like pertaining to the target building, as described in more detail below.

[0043] The ability to track collect and maintain secure information pertaining to one or more building rating systems for one or more target buildings over time may provide benefits to one or more participants of the lifecycle described above. For example, a building owner and/or subsequent purchaser, may be able to track what building rating systems have been performed for a target building, and data associated with each of those building rating systems, including, without limitation, information from inspectors as to whether the inspection was successful or not. As another example, certification organizations and/or inspectors can access building information and/or certification information pertaining to materials, structures, assemblies, and/or design of a target building and use this information in performance of one or more building rating system reviews without concern that such information has been altered or modified after it was provided.

[0044] FIG. 2 illustrates an example building management system according to an embodiment. As illustrated in FIG. 2, a system **200** may include one or more host electronic

devices **204a-N** and one or more client electronic devices **202a-N**. A host electronic device **204a-N** may be located remotely from a client electronic device **202a-N**. A server is an example of a host electronic device **204a-N** according to an embodiment. A host electronic device **204a-N** may have or be in communication with one or more data stores **206a-N**. In various embodiments, a host electronic device **204a-N** may include or be in communication with a rights management system **220**.

[0045] A host electronic device **204a-N** may be in communication with one or more client electronic devices **202a-N** over one or more communication networks **208a-N**. A communication network **208a-N** may be a local area network (LAN), a wide area network (WAN), a mobile or cellular communication network, an extranet, an intranet, the Internet and/or the like.

[0046] In various embodiments, a client electronic device **202a-N** may be a portable electronic device such as, for example, a smartphone, a tablet, a laptop, a wearable and/or the like. In other embodiments, a client electronic device **202a-N** may be desktop computer or other electronic device.

[0047] A client electronic device **202a-N** may be associated with a particular participant or representative in the target building rating system lifecycle. For example, as illustrated in FIG. 2, one or more client electronic devices **202a-N** may be associated with a building owner **212**, a certifier **214**, a certification organization **216**, an inspector **218**, a potential purchaser **222**, and/or the like.

[0048] As illustrated by FIG. 2, one or more host electronic devices **204a-N** may have access to one or more blockchains **210a-N**. The one or more blockchains may be used to manage information pertaining to one or more building rating systems for one or more target buildings

over a period of time, as described throughout this disclosure. The one or more host electronic devices **204a-N** may read, write, query, and/or otherwise access the blockchain. For example, the one or more host electronic devices may create new blocks on the blockchain, access the blockchain, and/or retrieve information from the blockchain in response to receiving requests from one or more client electronic devices.

[0049] As illustrated by FIG. 2, one or more host electronic devices **204a-N** may include or be in communication with a rights management system **220**. A rights management system **220** may include one or more electronic devices and/or one or more data stores. A rights management system **220** may maintain and/or implement one or more access policies that are applicable to the blockchain as explained in more detail below.

[0050] FIG. 3 illustrates an example blockchain data structure according to an embodiment. A blockchain **300a-N** includes one or more blocks **302a-N**. Optionally, a block may include one or more log records **304a-N**. As new log records are generated, a corresponding data representation of those log records may be added to the blockchain **300a-N** as part of a new block. As such, blocks **302a-N** of a blockchain **300a-N** may be positioned in a linear, sequential order. For example, blocks may be arranged in a chronological order. Blocks **302a-N** in a blockchain **300a-N** are linked to preceding blocks in the chain as illustrated in FIG. 3.

[0051] Optionally, one or more blocks **302a-N** of a blockchain **300a-N** may occupy the same data store or memory space. Alternatively, a blockchain **300a-N** may be implemented as via a distributed data store. For instance, blocks **302a-N** of a blockchain **300a-N** may not occupy the same data store or memory space, but rather two or more blocks in a blockchain may be implemented as distributed data stores. These distributed data stores may exist amongst remote electronic devices. For instance, part of a blockchain **300a-N** may be stored in a data store that is

associated with a first electronic device in a first location, while a different part of the blockchain may be stored in a different data store that is associated with a second electronic device in a second location that is different from the first location.

[0052] A block **302a-N** of a blockchain **300a-N** may be located in a data store at a first location, while a second block of the blockchain may be located in a data store at a second location. Despite remote storage proximity to one another, the blocks **302a-N** may still form the blockchain **300a-N** as they are linked to one another such as, for example, by way of their signatures.

[0053] In various embodiments, one or more participants of the system (e.g., building owners, certifiers, certification organizations, inspectors, potential purchasers, and/or other authorized users) may have a key pair that each may use to communicate and/or verify or authenticate communications and other information shared throughout the system. The key pair may include a private key and a public key associated with each participant. For example, if Building Owner A and Building Owner B are participants of the system, each may be associated with its own public/private key pair $\{ K_{pu}, K_{pr}\}$.

[0054] A participant may generate its own public and private keys. For example, a system associated with a participant may include a key generator, such as, for example, a random key generator, which may generate a public/private key pair for the participant. All client electronic devices associated with the participant may utilize the same public/private key pair in its communications with the system in order to uniquely authenticate itself as part of the participant's network. It is understood that client electronic devices associated with a participant may utilize different public/private key pairs in some embodiments, each associated with the participant. In various embodiments, one or more electronic devices associated with a participant

(e.g., one or more client electronic devices) may store a generated key pair in a secure data store associated with such device.

[0055] In various embodiments, each participant of the system may provide its public key with the system. The system may store one or more public keys and an indication of the participant to which it belongs in one or more data stores such as, for example, a key store. As explained in more detail below, the system may utilize a key store to authenticate communications via the system.

[0056] FIG. 4 illustrates a flow chart of an example method of securing the integrity of information provided as part of a building rating system review for a target building through tamper-evident logging according to an embodiment. Tamper-evident logging refers to a process that makes changes, modifications or access to log records easily detectable. This is true for modifications or changes made by unauthorized users who have no privileges on the system, as well as authorized users of the system.

[0057] In various embodiments, the system may identify one or more building owners. A system may identify one or more building owners In various embodiments, a listing of one or more building owners may be stored in a data store associated with or accessible by a host electronic device.

[0058] As illustrated by FIG. 4A, the system may receive **400** a communication from one or more building owners. For instance, a host electronic device may receive **400** an electronic communication from one or more client electronic devices associated with a building owner. The communication may include building information. This building information may be provided by a building owner as part of the construction or renovation of a target building. In other embodiments, building information may be provided by a building owner after the completion of

construction or renovation of a target building, or separate and apart from the development or renovation of a target building. In various embodiments, at least a portion of the building information provided by a building owner may be stored in a data store associated with or accessible by a host electronic device.

[0059] In various embodiments, the received communication may include message content and a digital signature. The message content may be building information. The system may use the digital signature to confirm that the communication actually came from the building owner.

[0060] A building owner may generate a digital signature for a communication by performing one or more cryptographic operations on at least a portion of the message content. For example, a building owner may generate a digital signature for a communication by generating, by an electronic device, a hash of at least a portion of the message content to generate a hashed value. For instance, a building owner that is sending building information may generate a hashed value corresponding to the building information by applying one or more hashing algorithms to the building information. The building owner may encrypt the hashed value with the building owner's private key to generate a digital signature corresponding to the message content.

[0061] The building owner may send the communication and corresponding digital signature to the system. In various embodiments, the system may authenticate **402** the received communication. Authenticating the communication may involve verifying that the communication originated from an authorized source such as, for example, an authorized building owner. In this way, only authorized building owner may request that information be added to a target blockchain, and users or those who access the target blockchain can be

confident that the target blockchain only includes relevant data. Authenticating the received communication may also involve confirming that the message content was not altered, modified or otherwise changed after it was sent.

[0062] The system may decrypt the received digital signature using the building owner's public key to yield a decrypted value. The decrypted value may be the received hashed value. If the decryption is successful, the system will know that the communication originated with the building owner. If the decryption is not successful, the system may disregard the communication.

[0063] The system may also verify the integrity of the message content. The system may apply the same hashing algorithm(s) used by the building owner to the received message content to generate a hashed value. The system may compare the hashed value it generated to the received hashed value. If the two values are the same, the system has verified that the message content has not changed since it was sent. If the values do not match, the system may disregard the communication as the message content has been changed after it was sent.

[0064] The system may create **404** a log file that includes at least a portion of the received building information. The log file may store the received building information in association with one or more target buildings, so that the building information is correlated to the target building to which it corresponds. The system may generate **406** a new block for a blockchain. The system may store the created log file in the new block.

[0065] In various embodiments, if a target blockchain already exists, the system may generate **406** a block to append to the end of the target blockchain. The target blockchain may store information about a target building through its rating system lifecycle. Additional and/or other target blockchains may be used within the scope of this disclosure.

[0066] Referring back to FIG. 4A, the system may add **408** the new block to a target blockchain. If the target blockchain already exists, the system may identify the last block of the target blockchain. The last block may be associated with a signature. The signature may be derived or based on a signature of a block that precedes the last block in the target blockchain. The preceding block may immediately precede the last block in the target blockchain, or it may not immediately precede the last block but be separated from the target block by one or more other blocks.

[0067] For instance, the signature of the last block may be a result of one or more cryptographic operations, such as, for example, a hash function, performed on at least a portion of the contents of a block that precedes the last block in the target blockchain. As such, the blocks of the blockchain may be inextricably linked together, and modification of one block will require modification of the previous blocks in the chain.

[0068] The system may add **408** the new block to the target blockchain by performing one or more cryptographic operations on at least a portion of the content of the last block in the target blockchain to generate a signature. The system may add the signature to the new block and append it the end of the target blockchain. For instance, the system may link the new block to the last block of the target blockchain.

[0069] If a target blockchain does not already exist, the system may generate a first block of a blockchain. If the generated block is also the only block in the target blockchain, then the signature of the block may not be based on a preceding block because there is no preceding block in the chain. In this situation, the signature of the block may be a result of one or more cryptographic operations performed on at least part of the block, such as, for example, a portion of the block's log records.

[0070] In various embodiments, the system may maintain a source log that tracks which blocks are associated with which participant in the lifecycle. For instance, if the system receives building information from Building Owner 1 to add to the target block chain for a target building, the system may assign a unique identifier to Building Owner 1. The system may update a source log to associate one or more generated blocks with the source of the information stored within the block. For instance, the system may assign Building Owner 1 the unique identifier "02d3" and may store in the source log an indication of the newly created block associated with Building Owner 1. This indication may be the signature of or other unique identifier associated with the newly created block. FIG. 5 illustrates an example of a source log according to an embodiment.

[0071] In various embodiments, the system may identify one or more certifiers. A listing of one or more certifiers may be stored in a data store associated with or accessible by a host electronic device. The listing may correlate one or more certifiers to one or more building owners according to an embodiment.

[0072] Referring back to FIG. 4A, the system may receive **410** a communication from one or more certifiers. For instance, a host electronic device may receive **410** an electronic communication from one or more client electronic devices associated with a certifier. The communication may include certification information. This certification information may be provided by a certifier as part of the construction or renovation of a target building. In other embodiments, certification information may be provided by a certifier after the completion of construction or renovation of a target building, or separate and apart from the development or renovation of a target building. In various embodiments, at least a portion of the building

information provided by a certifier may be stored in a data store associated with or accessible by a host electronic device.

[0073] The information that is provided by a certifier (e.g., certification information), may be uniquely correlated with a target building or one or more components or portions thereof, for example, by a unique identifier.

[0074] In various embodiments, the received communication may include message content and a digital signature. The message content may be certification information corresponding to a target building or one or more components or portions thereof. The system may use the digital signature to confirm that the communication actually came from the certifier.

[0075] A certifier may generate a digital signature for a communication by performing one or more cryptographic operations on at least a portion of the message content. For example, a certifier may generate a digital signature for a communication by generating, by an electronic device, a hash of at least a portion of the message content to generate a hashed value. For instance, a certifier that is sending certification information for a target building may generate a hashed value corresponding to the certification information by applying one or more hashing algorithms to the certification information. The certifier may encrypt the hashed value with the certifier's private key to generate a digital signature corresponding to the message content.

[0076] The certifier may send the communication and corresponding digital signature to the system. In various embodiments, the system may authenticate **412** the received communication. Authenticating the communication may involve verifying that the communication originated from an authorized source such as, for example, an authorized certifier. In this way, only authorized certifiers may request that information be added to a target blockchain, and users or those who access the target blockchain can be confident that the target

blockchain only includes relevant data. Authenticating the received communication may also involve confirming that the message content was not altered, modified or otherwise changed after it was sent.

[0077] The system may decrypt the received digital signature using the certifier's public key to yield a decrypted value. The decrypted value may be the received hashed value. If the decryption is successful, the system will know that the communication originated with the certifier. If the decryption is not successful, the system may disregard the communication.

[0078] The system may also verify the integrity of the message content. The system may apply the same hashing algorithm(s) used by the certifier to the received message content to generate a hashed value. The system may compare the hashed value it generated to the received hashed value. If the two values are the same, the system has verified that the message content has not changed since it was sent. If the values do not match, the system may disregard the communication as the message content has been changed after it was sent.

[0079] The system may create **414** a log file that includes at least a portion of the received certification information. The log file may store the received certification information in association with one or more target buildings, so that the certification information is correlated to the target building to which it corresponds. The system may generate **416** a new block for a blockchain. The system may store the created log file in the new block.

[0080] In various embodiments, if a target blockchain already exists, the system may generate **416** a block to append to the end of the target blockchain. For example, the target blockchain may store information about a target building or one or more components thereof throughout its lifecycle. Additional and/or other target blockchains may be used within the scope of this disclosure.

[0081] Referring back to FIG. 4A, the system may add **418** the new block to a target blockchain. If the target blockchain already exists, the system may identify the last block of the target blockchain. The last block may be associated with a signature. The signature may be derived or based on a signature of a block that precedes the last block in the target blockchain. The preceding block may immediately precede the last block in the target blockchain, or it may not immediately precede the last block but be separated from the target block by one or more other blocks.

[0082] For instance, the signature of the last block may be a result of one or more cryptographic operations, such as, for example, a hash function, performed on at least a portion of the contents of a block that precedes the last block in the target blockchain. As such, the blocks of the blockchain may be inextricably linked together, and modification of one block will require modification of the previous blocks in the chain.

[0083] The system may add **418** the new block to the target blockchain by performing one or more cryptographic operations on at least a portion of the content of the last block in the target blockchain to generate a signature. The system may add the signature to the new block and append it the end of the target blockchain. For instance, the system may link the new block to the last block of the target blockchain.

[0084] If a target blockchain does not already exist, the system may generate a first block of a blockchain. If the generated block is also the only block in the target blockchain, then the signature of the block may not be based on a preceding block because there is no preceding block in the chain. In this situation, the signature of the block may be a result of one or more cryptographic operations performed on at least part of the block, such as, for example, a portion of the block's log records.

[0085] In various embodiments, the system may maintain a source log that tracks which blocks are associated with which participant in the lifecycles. For instance, if the system receives quality data from Certifier 1 to add to the target block chain for a target building, the system may assign a unique identifier to Certifier 1. The system may update a source log to associate one or more generated blocks with the source of the information stored within the block. For instance, the system may assign Certifier 1 the unique identifier "024v3" and may store in the source log an indication of the newly created block associated with Certifier 1. This indication may be the signature of or other unique identifier associated with the newly created block.

[0086] In various embodiments, the system may receive **420** a communication from one or more certification organizations. For instance, a host electronic device may receive **420** an electronic communication from one or more client electronic devices associated with a certification organization. The communication may include administration information corresponding to one or more building rating systems for a target building.

[0087] The information that is provided by a certification organization (e.g., administration information) may be uniquely correlated with one or more target buildings, for example, by a unique identifier.

[0088] In various embodiments, the received communication may include message content and a digital signature. The message content may be administration information, corresponding to one or more target buildings. The system may use the digital signature to confirm that the communication actually came from the certification organization.

[0089] A certification organization may generate a digital signature for a communication by performing one or more cryptographic operations on at least a portion of the message content. For example, a certification organization may generate a digital signature for a communication

by generating, by an electronic device, a hash of at least a portion of the message content to generate a hashed value. For instance, a certification organization that is sending administration information may generate a hashed value corresponding to the data by applying one or more hashing algorithms to the data. The certification organization may encrypt the hashed value with the certification organization's private key to generate a digital signature corresponding to the message content.

[0090] The certification organization may send the communication and corresponding digital signature to the system. In various embodiments, the system may authenticate **422** the received communication. Authenticating the communication may involve verifying that the communication originated from an authorized source such as, for example, an authorized certification organization. In this way, only authorized certification organizations may request that information be added to a target blockchain, and users or those who access the target blockchain can be confident that the target blockchain only includes relevant data. Authenticating the received communication may also involve confirming that the message content wasn't altered, modified or otherwise changed after it was sent.

[0091] The system may decrypt the received digital signature using the certification organization's public key to yield a decrypted value. The decrypted value may be the received hashed value. If the decryption is successful, the system will know that the communication originated with the certification organization. If the decryption is not successful, the system may disregard the communication.

[0092] The system may also verify the integrity of the message content. The system may apply the same hashing algorithm(s) used by the certification organization to the received message content to generate a hashed value. The system may compare the hashed value it

generated to the received hashed value. If the two values are the same, the system has verified that the message content has not changed since it was sent. If the values do not match, the system may disregard the communication as the message content has been changed after it was sent.

[0093] The system may create **424** a log file that includes at least a portion of the received administration information. The log file may store the received administration information in association with one or more target buildings, so that the administration information is correlated to the target building to which it corresponds.

[0094] The system may generate **426** a new block for the target blockchain. The system may store the created log file in the new block. In various embodiments, the system may add **428** the new block to the target blockchain. For example, the system may add **428** the new block to the target blockchain in a manner similar to that described above.

[0095] The system may update the source log to associate with generated certification organization block with the certification organization that provided the corresponding administration information. For instance, the system may assign Certification Organization 1 the unique identifier “u9ra” and may store in the source log an indication of the newly created block associated with Certification Organization 1. This indication may be the signature of or other unique identifier associated with the newly created block.

[0096] In various embodiments, the system may identify one or more inspectors of one or more target buildings. The system may access a list of inspectors from one or more data stores associated with or accessible by a host electronic device. An inspector may be associated with one or more certification organizations. By knowing which certification organization was administering a building rating system for a target building, the system may access a

corresponding list of inspectors associated with the certification organization from one or more data stores.

[0097] The system may receive **430** a communication from one or more of the identified inspectors. For instance, a host electronic device may receive **430** an electronic communication from one or more client electronic devices associated with an inspector. The communication may include inspection information associated with a target building.

[0098] In various embodiments, the received communication may include message content and a digital signature. The message content may be inspection information. The system may use the digital signature to confirm that the communication actually came from the inspector.

[0099] An inspector may generate a digital signature for a communication by performing one or more cryptographic operations on at least a portion of the message content. For example, an inspector may generate a digital signature for a communication by generating, by an electronic device, a hash of at least a portion of the message content to generate a hashed value. For instance, an inspector that is sending installation data may generate a hashed value corresponding to the data by applying one or more hashing algorithms to the data. The inspector may encrypt the hashed value with the inspector's private key to generate a digital signature corresponding to the message content.

[00100] The inspector may send the communication and corresponding digital signature to the system. In various embodiments, the system may authenticate **432** the received communication. Authenticating the communication may involve verifying that the communication originated from an authorized source such as, for example, an identified inspector (or an otherwise authorized inspector). In this way, only authorized inspectors may

request that information be added to a target blockchain, and users or those who access the target blockchain can be confident that the target blockchain only includes relevant data. Authenticating the received communication may also involve confirming that the message content was not altered, modified or otherwise changed after it was sent.

[00101] The system may decrypt the received digital signature using the inspector's public key to yield a decrypted value. The decrypted value may be the received hashed value. If the decryption is successful, the system will know that the communication originated with the installer. If the decryption is not successful, the system may disregard the communication.

[00102] The system may also verify the integrity of the message content. The system may apply the same hashing algorithm(s) used by the inspector to the received message content to generate a hashed value. The system may compare the hashed value it generated to the received hashed value. If the two values are the same, the system has verified that the message content has not changed since it was sent. If the values do not match, the system may disregard the communication as the message content has been changed after it was sent.

[00103] The system may authenticate **432** a received communication using cryptography. For example, the system may verify that a received communication was sent by a known or authorized inspector by confirming that the communication was encrypted using the installer's private key. For example, in response to receiving a communication from an inspector, the system may retrieve that inspector's public key from the key store. The system may attempt to decrypt the received communication using the retrieved public key. If the retrieved public key is successful in decrypting the communication, the system can be confident that the communication originated from the authorized inspector. If the retrieved public key is not successful in decrypting the communication, the system may discard the communication

since it was not sent from the purported inspector. Additional and/or alternate authentication protocols may be used within the scope of this disclosure.

[00104] The system may create **434** a log file that includes at least a portion of the received inspection information. The log file may store the received inspection information in association with one or more target buildings, so that the inspection information is correlated to the target building to which it corresponds.

[00105] The system may generate **436** a new block for the target blockchain. The system may store the created log file in the new block. In various embodiments, the system may add **438** the new block to the target blockchain. For example, the system may add **438** the new block to the target blockchain in a manner similar to that described above.

[00106] The system may update the source log to associate with generated inspector block with the inspector that provided the corresponding inspection information. For instance, the system may assign Inspector 1 the unique identifier "lx2h" and may store in the source log an indication of the newly created block associated with Inspector 1. This indication may be the signature of or other unique identifier associated with the newly created block.

[00107] In various embodiments, at least a portion of the target blockchain may be accessible by one or more of the identified participants, such as, for example, building owners, certifiers, certification organizations, inspectors, potential purchasers, and/or the like. As described in more detail below, one or more participants may query or request information that is stored in the target blockchain.

[00108] One or more host electronic devices may receive one or more access requests. An access request may include a request to access certain information that is stored on the target blockchain. For instance, an access request may be a request to access information associated

with a particular target building or component thereof. As another example, an access request may be a request to access information about one or more building rating system reviews performed for a target building. Additional and/or alternate access requests may be made within the scope of this disclosure.

[00109] An access request may originate from a participant (e.g., a building owner, a certifier, a certification organization, an inspector, a potential purchaser, and/or the like) and/or one or more authorized business partners of one or more participants. However, the system may only grant access to requested information if it is permitted by an access policy associated with the target blockchain. An access policy is a list, table, or other data structure that identifies privileges or permissions that apply to a particular resource or set of resources.

[00110] An access control list (ACL) is an example of an access policy according to an embodiment. A blockchain is another example of an access policy according to an embodiment. For example, one or more permissions and associated requestors may be stored on an access control blockchain. The access control blockchain may be separate from the target blockchain. A host electronic device may access an access control blockchain in order to determine whether a requestor has the requisite permissions to access the requested resources from the target blockchain. For example, an access control blockchain may include one or more blocks with one or more access rights associated with one or more of the resources and/or one or more authorized users of the target blockchain.

[00111] An access policy may define one or more permissions associated with one or more authorized users of the target blockchain. In various embodiments, the access policy may define one or more permissions based on type of authorized users, for example, building owners, certifiers, certification organizations, inspectors, or potential purchasers. Alternatively, an access

policy may define one or more permissions to one or more users on a case-by-case basis. Example permissions may include, without limitation, read access, write access, copy permission, download permission, and/or the like.

[00112] A rights management system may restrict access to one or more blockchains and/or information stored by one or more blockchains in accordance with one or more applicable access policies. For example, a rights management system may control who can access what information on a blockchain and for what purposes this information may be accessed or further utilized. For instance, a certifier may access building information for a building owner on whose behalf the certifier is working. However, the certifier may not access data of a different building owner.

[00113] As another example, a potential purchaser may access inspection data for a target building that it is considering purchasing (e.g., one that is under contract), but the potential purchaser may not have access to inspection data for other buildings.

[00114] FIG. 6A illustrates a flow chart of an example method of verifying access requests to a target blockchain according to an embodiment. As illustrated by FIG. 6A, a host electronic device may receive **600** an access request from a requestor. In various embodiments, a requestor may be a building owner, a certifier, a certification organization, an inspector, a potential purchaser, another authorized user, and/or the like. The access request may include an indicator of one or more resources stored on the blockchain for which access is sought. A resource refers to information pertaining to the supply, manufacturer, installation, inspection, use, and/or performance of one or more components of a target building having information that is stored on a target blockchain. A resource may be information itself or one or more log records

that includes such information. The resources may be identified based on the source of the access request.

[00115] For example, information associated with a component of a target building may be stored and/or indexed according to a unique identifier. Information stored on the blockchain pertaining to the component may be stored in association with its unique identifier.

[00116] The host electronic device may identify **602** one or more blocks of the target blockchain that include at least a portion of the resources. For example, if an inspector would like to know if the characteristics of a component comply with one or more requirements of a building rating system, the inspector may query the blockchain for relevant data pertaining to the component to verify compliance. For example, an inspector may query the blockchain to determine the dates and reports from any previous inspections that may have been conducted.

[00117] The host electronic device may identify **604** the access policy that corresponds to the target blockchain, and may determine **606**, based on the access policy whether the requestor is permitted to access the requested resources. For instance, the host electronic device may search the access policy for the requestor's identity, and may obtain the permissions granted to the requestor. If the request being made by the requestor is permitted by the policy, the host electronic device may grant **608** access to the requested resources to the requestor. Otherwise, the host electronic device may deny **610** access.

[00118] As an example, Building Owner A may make an access request to obtain building information associated with a target building and that is stored on a target blockchain. The access policy for the target blockchain may indicate that Building Owner A is permitted to access its own information (e.g., information that it provided to the target blockchain), and therefore may grant access to the requesting building owner. However, if Building Owner A

attempts to access building information associated with a different building owned by Building Owner B, the system may deny the request.

[00119] In various embodiments, the system may determine a unique identifier associated with a requestor. If the unique identifier of the requestor does not match a unique identifier associated with the creator of block for which access is being sought (as specified, for example, by the source log), the system may deny the request. If the unique identifier of the requestor matches a unique identifier associated with the creator of the block for which access is being sought, the system may grant the request.

[00120] The types of queries of a target blockchain that may be made may vary based on the user or type of user requesting the query. For example, a building owner and/or certifier may submit a query to a host electronic device for access to a specification report for one or more components of a target building. As another example, a building owner and/or certifier may query for information pertaining to a certification organization's building rating information. As yet another example of querying, an inspector may query building information provided by a building owner, certification information provided by a certifier, and/or administration information of a certification organization to assess compliance of a target building or component thereof with one or more applicable building rating system requirements.

[00121] FIGS. 6B-6C show a visual depiction of example access requests according to various embodiments. As shown in FIG. 6B, a portion of an example blockchain **612** includes two building owner blocks **614**, **616**, two certifier blocks **618**, **620**, two certification organization blocks **622**, **624**, and two inspector blocks **626**, **628**. It is understood that different numbers of one or more such blocks may be used within the scope of this disclosure.

[00122] In this example, Building Owner A has shared building information pertaining to Building A to the blockchain. As such, the system may grant a request by Building Owner A to access this building information because the access rights may permit Building Owner A to access information that it has supplied to the blockchain **612**.

[00123] In this example, Building Owner B has shared building information pertaining to Building B to the blockchain **612**. As such, the system may deny a request by Building Owner A to access this building information because the access rights may prohibit Building Owner A from accessing this information.

[00124] As another example, Inspector B may be performing a certification inspector of Building B for compliance with a building rating system administered by Certification Organization B. As part of this inspection, Inspector B may be allowed to access building information and certification information associated with Building B. However, Inspector B may be prohibited from accessing certification information for Building A.

[00125] As another example, Potential Purchaser A may be under contract to purchase Building A. As part of its diligence, Potential Purchaser A may be permitted to access inspection data associated with Building A. However, Potential Purchaser A may be prohibited from accessing inspection data associated with Building B.

[00126] It is understood that additional and/or alternate access examples, access rights, participants, and/or the like may be used within the scope of this disclosure.

[00127] For example, a building inspector may access certification information for a building, as well as past inspection reports, to determine an on-going certification compliance for a building.

[00128] In various embodiments, an authorized blockchain participant may delegate one or more of its access rights to the blockchain to one or more business partners. A business partner refers to an entity, organization, or individual with whom a participant has a business or other relationship. Examples of business partners include, without limitation, customers, clients, partners, manufacturers, installers, inspectors, suppliers, distributors, vendors, agents, affiliates, subsidiaries, contractors, and/or the like.

[00129] For example, a building owner may delegate one or more of its blockchain access rights to one or more of its property managers or subcontractors. Similarly, an authorized certifier may delegate one or more of its blockchain access rights to one or more of its agents, and/or other partners. A certification organization may delegate one or more of its blockchain access rights to one or more inspectors.

[00130] FIG. 7 illustrates an example delegation process according to an embodiment. As illustrated by FIG. 7, the system may generate **700** a token for one or more authorized participants. For example, when an authorized user registers with, enrolls with, and/or accesses the system, the system may generate **700** one or more tokens for the user. A token refers to an object that includes an identifier associated with the user and one or more blockchain access rights granted to that user. In various embodiments, a token may include an indication of the information or resources on a blockchain to which one or more of the access rights apply or correspond. For instance, a participant may have a first set of access rights to a first set of information that is on a blockchain, but a second set of access rights to a second set of information that is stored on the blockchain. A token that is generated for the participant may include a listing of such access rights and information or resources to which each of the access rights apply. Alternatively, the system may generate **700** multiple tokens for a participant, each

token corresponding to particular information from the blockchain and one or more applicable access rights.

[00131] For example, FIGS. 9A and 9B illustrate two sets of building information that a building owner may store on a blockchain. The system may generate a token **902** that corresponds to both sets of building information (or at least a portion of both sets) as illustrated in FIG. 9A. As illustrated in FIG. 9A, the token may identify a particular subset of the building information and one or more access rights associated with the subset. In various embodiments, one or more access rights may apply to the building information as a whole rather than on a subset-by-subset basis.

[00132] In other embodiments, the system may generate multiple tokens **904a**, **904b** as illustrated in FIG. 9B. As shown in FIG. 9B, one token **904a** corresponds to the access rights associated with one set of information (Building Information 1), while another token **904b** corresponds to access rights associated with another set of information (Building Information 2). It is understood that additional and/or alternate tokens, information, access rights and/or the like may be used within the scope of this disclosure.

[00133] The access rights and information to which they correspond may be determined based on those reflected in one or more access policies associated with the blockchain, as described above. In various embodiments, the access rights may include an indication as to whether a user may delegate one or more access rights may be delegated. The indication may also indicate which access the rights the user may delegate, which information stored on the blockchain such rights may be delegated, how many tiers of delegation are permitted, and/or the like. For example, FIG. 7 illustrates a single tier of delegation (from a participant to one or more business partners). But, in certain embodiments, a participant may be able to delegate one or

more rights through multiple tiers of business partners. FIG. 8 illustrates an illustration of an example multiple-tier delegation process according to an embodiment. As illustrated in FIG. 8, a system **800** may issue a token to a participant **802**. The participant **802** may delegate one or more of its access rights to access certain information Business Partner 1 **804** and Business Partner 2 **806**. For example, as illustrated in FIG. 8, participant **802** may delegate access rights A and B to Info A Business Partner 1 **804**, and access rights C and D to Info A Business Partner 2 **806**. It is understood that additional or alternate right delegations or combinations of delegations may be made within the scope of this disclosure. As illustrated in FIG. 8, this may be considered a single tier of delegation.

[00134] Business Partner 1 **804** in turn may delegate at least a portion of its access rights for Info A to Business Partner 3 **808**, while Business Partner 2 **806** may delegate at least a portion of its access rights for Info A to Business Partner 4 **810** and Business Partner 5 **812**. As illustrated in FIG. 8, this may be considered a second tier of delegation. Although FIG. 8 illustrates two delegation tiers, it is understood that additional or fewer tiers of delegation may be used within the scope of this disclosure.

[00135] Referring back to FIG. 7, the system may send **702** the generated token to the authorized participant. The authorized participant may receive the token and store **704** the token. In some embodiments, the participant may send the token as part of a communication to the system. For example, a participant may send its token to the system along with an access request. In some embodiments, the system may determine what access rights the participant has based on the received token. In other embodiments, the system may confirm that the access rights denoted in the received token align with the access rights maintained by the system (e.g., those of one or more access policies).

[00136] A participant may generate **706** a digital signature for a token by generating, by an electronic device, a hash of at least a portion of the token to generate a hashed value. The participant may encrypt the hashed value with the participant's private key to generate a digital signature corresponding to the message content.

[00137] A participant may delegate one or more of its access rights to a business partner by providing **708** the business partner with a delegated token and the digital signature corresponding to the delegated token. The delegated token may be the participant's token (or a portion thereof), a reference to the participant's token, a new token based on the participant's token, and/or the like. A participant may only delegate the access rights that it has for certain information. In this way, a participant cannot grant more rights to a delegate that it itself has.

[00138] For example, a building owner may have read access for a first set of building information that includes identification and installation information pertaining to a component of its building. The building owner may have read and modify access for a second set of building information that includes information about personnel at the building. The building owner may delegate its read access to the first set of building information and/or its read/modify access to the second set of building information to one of its property managers. However, the building owner may not delegate modify access to the second set of building information to the property manager because the building owner does not have this right. The delegated token may include an indication of the participant who delegated one or more access rights, and an indication of the one or more delegated access rights.

[00139] The participant may send the token and corresponding digital signature to a business partner. When the business partner makes an access request **710** to the system, it may include the delegated token and the received digital signature with the request. The system may

attempt to decrypt **712** the received digital signature using the participant's public key to yield a received hashed value. If the decryption is successful, the system will know that the token provided by the business partner was issued by the participant. If the decryption is not successful, the system may disregard the communication.

[00140] The system may also verify **714** the integrity of the token. The system may apply the same hashing algorithm(s) used by the participant to generate a hashed value. The system may compare the hashed value it generated to the received hashed value. If the two values are the same, the system has verified that the token has not changed since it was sent. If the values do not match, the system may disregard the communication as the token has been changed after it was sent.

[00141] The system may determine **716** whether the delegating participant has the right to delegate the access rights to the information being requested. For instance, the system may identify the delegating participant from the received token, and may confirm its delegation rights with one or more of the system access policies. If the system determines that the delegating participant does not have the necessary delegation rights for the information being requested, the system may deny the access request.

[00142] Referring to FIG. 4A, in various embodiments, the system may perform **440** one or more verification checks on of the target blockchain. The system may perform **440** one or more verification checks in response to one or more triggering events. A triggering event refers to an action performed on the target blockchain or a request made to the target blockchain. For example, if a request for a particular type of information is made to the target blockchain, the system may perform a verification check to determine whether the requested information is

consistent with other information logged at the target blockchain. Additional and/or alternate triggering events may be used within the scope of this disclosure.

[00143] In other embodiments, the system may perform **440** one or more verification checks at one or more regular intervals, or in response to a user requesting a verification check.

[00144] For example, an inspector may perform a verification check to ensure that a test performed is consistent with a building's rating. Additional and/or alternate types of comparisons may be performed within the scope of this disclosure.

[00145] In response to the verification check failing, the system may perform **442** one or more remedial actions. For example, in the above example, the system may automatically send one or more notifications if an inconsistency is detected. The notification may be an email or other electronic notification, and the system may send it to one or more applicable parties such as, for example, one or more participants of the system. For example, if a test performed by an inspector should fail to meet expectations, the system may automatically send one or more notifications to a building owner, a certification organization, or other business partner, or one or more other parties. For instance, a target blockchain may include administration information in one or more certification organization blocks that correspond to one or more building rating systems administered by a certification organization. The administration information may include one or more acceptable values and/or ranges of values associated with one or more tests that are performed as part of the building rating system. If an inspector performs a test and the result differs from an acceptable value or is outside of an acceptable range for that test, the system may send one or more notifications to a building owner, a certification organization, or other business partner.

[00146] Alternative remedial actions may include opening a case that includes a root cause analysis, making corrective action assignments, and/or identifying one or more proposed preventive measures. In various embodiments, one or more participants of the system may be able to contribute to identifying the root cause and/or proposed one or more corrective or remedial actions.

[00147] FIG. 10 depicts a block diagram of hardware that may be used to contain or implement program instructions, such as those of a cloud-based server, electronic device, virtual machine, or container. A bus **1000** serves as an information highway interconnecting the other illustrated components of the hardware. The bus may be a physical connection between elements of the system, or a wired or wireless communication system via which various elements of the system share data. Processor **1005** is a processing device that performs calculations and logic operations required to execute a program. Processor **1005**, alone or in conjunction with one or more of the other elements disclosed in FIG. 10, is an example of a processing device, computing device or processor as such terms are used within this disclosure. The processing device may be a physical processing device, a virtual device contained within another processing device, or a container included within a processing device.

[00148] A memory device **1020** is a hardware element or segment of a hardware element on which programming instructions, data, or both may be stored. Read only memory (ROM) and random access memory (RAM) constitute examples of memory devices, along with cloud storage services.

[00149] An optional display interface **1030** may permit information to be displayed on the display **1035** in audio, visual, graphic or alphanumeric format. Communication with external devices, such as a computing device, may occur using various communication devices **1040**,

such as a communication port or antenna. A communication device **1040** may be communicatively connected to a communication network, such as the Internet or an intranet.

[00150] The hardware may also include a user input interface **1045** which allows for receipt of data from input devices such as a keyboard or keypad **1050**, or other input device **1055** such as a mouse, a touch pad, a touch screen, a remote control, a pointing device, a video input device and/or a microphone. Data also may be received from an image capturing device **1010** such as a digital camera or video camera. A positional sensor **1015** and/or motion sensor **1065** may be included to detect position and movement of the device. Examples of motion sensors **1065** include gyroscopes or accelerometers. An example of a positional sensor **1015** is a global positioning system (GPS) sensor device that receives positional data from an external GPS network.

[00151] Various embodiments may include a computer-readable medium containing programming instructions that are configured to cause one or more processors to perform the functions described in the context of the previous figures.

[00152] The features and functions described above, as well as alternatives, may be combined into many other different systems or applications. Various alternatives, modifications, variations or improvements may be made by those skilled in the art, each of which is also intended to be encompassed by the disclosed embodiments.

CLAIMS

What Is Claimed Is:

1. A method of securing data associated with one or more building rating systems, the method comprising:

by one or more electronic devices:

receiving, from a building owner of a target building that is a subject of a building rating system, a communication comprising building information corresponding to the target building,

generating a building owner block that is associated with the building owner,

storing at least a portion of the building information in the building owner blocks,

adding the building owner block to a blockchain,

identifying a certifier associated with the target building,

receiving, from the identified certifier, a communication comprising certification information corresponding to the target building, wherein the certification information comprises at least a portion of the building information that the certifier has retrieved from the building owner block,

generating a certifier block that is associated with the identified certifier,

storing at least a portion of the certification information in the certifier block,

adding the certifier block to the blockchain,

identifying an inspector associated with a certification organization responsible for administering the building rating system,

receiving, from the identified inspector, a communication comprising inspection information corresponding to the target building, wherein the inspection information comprises information pertaining to compliance of the target building or one or more components of the target building with one or more requirements of the building rating system,

generating an inspection block that is associated with the identified inspector,

storing at least a portion of the inspection information in the inspection block,

adding the inspection block to the blockchain,

wherein at least a portion of the blockchain is accessible by the building owner, the certifier, the certification organization, and/or one the inspector according to an access policy associated with the blockchain, wherein the access policy includes an access control list that defines one or more access rights to the blockchain.

2. The method of claim 1, further comprising performing one or more of the following:

authenticating the communication from the building owner before adding the building owner block to the blockchain;

authenticating the communication from the identified certifier before adding the certifier block to the blockchain; or

authenticating the communication from the identified inspector before adding the inspection block to the blockchain.

.

3. The method of claim 2, wherein authenticating the communication from the building owner comprises:

receiving a digital signature in connection with the communication from the building owner;

retrieving a public key associated with the building owner from a key store; and

using the public key to decrypt the digital signature to yield a decrypted value.

4. The method of claim 3, further comprising:

applying a hashing algorithm to the communication from the building owner to yield a hashed value;

determining whether the hashed value matches the decrypted value; and

in response to determining that the hashed value matches the decrypted value, adding the building owner block to the blockchain.

5. The method of claim 2, wherein authenticating the communication from the identified certifier comprises:

receiving a digital signature in connection with the communication from the identified certifier;

retrieving a public key associated with the identified certifier from a key store; and

using the public key to decrypt the digital signature to yield a decrypted value.

6. The method of claim 5, further comprising:

applying a hashing algorithm to the communication from the identified certifier to yield a hashed value;

determining whether the hashed value matches the decrypted value; and

in response to determining that the hashed value matches the decrypted value, adding the certifier block to the blockchain.

7. The method of claim 2, wherein authenticating the communication from the identified inspector comprises:

receiving a digital signature in connection with the communication from the identified inspector;

retrieving a public key associated with the identified inspector from a key store; and

using the public key to decrypt the digital signature to yield a decrypted value.

8. The method of claim 7, further comprising:

applying a hashing algorithm to the communication from the identified inspector to yield a hashed value;

determining whether the hashed value matches the decrypted value; and

in response to determining that the hashed value matches the decrypted value, adding the inspection block to the blockchain.

9. The method of claim 1, further comprising:

receiving, from the certification organization, a communication comprising administration information associated with the building rating system;

generating certification organization block that is associated with the certification organization;

storing at least a portion of the administration information in the certification organization block of the certification organization;

adding the certification organization block to the blockchain, and

wherein at least a portion of the blockchain is accessible by the certification organization according to the one or more access rights.

10. The method of claim 9, further comprising:

generating a token for the certification organization, wherein the token comprises:

an identifier associated with the certification organization,

one or more of the one or more access rights that correspond to the certification organization, and

for each of the access rights that correspond to the certification organization, an indication of a subset of information that is stored on the blockchain to which the access right corresponds; and

sending the token to the certification organization.

11. The method of claim 10, wherein the token further comprises:

an indication of which of the access rights that correspond to the certification organization the certification organization can delegate to one or more business partners for each of the subsets of information that to which the access rights corresponds.

12. The method of claim 10, wherein the token further comprises an indication of how many tiers of delegation the certification organization is permitted to make.

13. The method of claim 10, further comprising:

by an electronic device associated with the certification organization:

generating a delegated token for a business partner that comprises:

an indication of one or more delegated access rights, wherein the delegated access rights comprise one or more of the access rights that correspond to the certification organization, and

for each of the delegated access rights, an indication of at least a portion of the subset of information that is stored on the blockchain to which the delegated access rights correspond.

14. The method of claim 13, further comprising:

by the electronic device associated with the certification organization:

generating a digital signature associated with the delegated token, and

sending the delegated token and the digital signature to the certification organization.

15. The method of claim 14, wherein generating a digital signature associated with the delegated token comprises:

applying a hashing algorithm to at least a portion of the delegated token to yield a hashed value; and

encrypting the hashed value with a private key associated with the certification organization.

16. The method of claim 1, further comprising:

receiving an access request from the building owner, wherein the access request comprises an indication of one or more resources stored on the blockchain for which access is sought;

determining one or more blocks of the blockchain that include at least a portion of the resources;

determining, based on the access policy, whether the building owner is permitted to access the one or more resources; and

in response to determining that the building owner is permitted to access the one or more resources, providing access to the one or more resources to the building owner.

17. The method of claim 16, further comprising accessing a second blockchain that comprises one or more second blocks, wherein each of the one or more second blocks comprises one or more access rights associated with one or more of the resources and/or one or more authorized users of the blockchain.

18. The method of claim 16, wherein:

the one or more resources correspond to the building owner,

determining whether the building owner is permitted to access the one or more resources comprises determining that the building owner is permitted to access the one or more resources.

19. The method of claim 16, wherein:

the one or more resources correspond to one or more other building owners,

determining whether the building owner is permitted to access the one or more resources comprises determining that the building owner is not permitted to access the one or more resources.

20. The method of claim 1, further comprising:

receiving an access request from the identified certifier, wherein the access request comprises an indication of one or more resources stored on the blockchain for which access is sought;

determining one or more blocks of the blockchain that include at least a portion of the resources;

determining, based on the access policy, whether the identified certifier is permitted to access the one or more resources; and

in response to determining that the identified certifier is permitted to access the one or more resources, providing access to the one or more resources to the identified certifier.

21. The method of claim 20, further comprising accessing a second blockchain that comprises one or more second blocks, wherein each of the one or more second blocks comprises one or more access rights associated with one or more of the resources and/or one or more authorized users of the blockchain.

22. The method of claim 20, wherein:

the one or more resources correspond to the identifier certifier,

determining whether the identifier certifier is permitted to access the one or more resources comprises determining that the identifier certifier is permitted to access the one or more resources.

23. The method of claim 20, wherein:

the one or more resources correspond to one or more other certifiers,

determining whether the identifier certifier is permitted to access the one or more resources comprises determining that the identified identifier certifier is not permitted to access the one or more resources.

24. The method of claim 1, further comprising:

receiving an access request from the identified inspector, wherein the access request comprises an indication of one or more resources stored on the blockchain for which access is sought;

determining one or more blocks of the blockchain that include at least a portion of the resources;

determining, based on the access policy, whether the identified inspector is permitted to access the one or more resources; and

in response to determining that the identified inspector is permitted to access the one or more resources, providing access to the one or more resources to the identified inspector.

25. The method of claim 24, wherein:

the one or more resources correspond to a second inspector who is not associated with the certification organization,

determining whether the identified inspector is permitted to access the one or more resources comprises determining that the identified inspector is not permitted to access the one or more resources.

26. The method of claim 24, wherein:

the one or more resources correspond to one or more certifiers who provided certification information to the identified inspector;

determining whether the identified inspector is permitted to access the one or more resources comprises determining that the inspector is permitted to access the one or more resources.

27. The method of claim 24, wherein:

the one or more resources correspond to one or more certifiers who did not provide certification information to the identified inspector;

determining whether the identified inspector is permitted to access the one or more resources comprises determining that the identified inspector is not permitted to access the one or more resources.

28. The method of claim 24, further comprising accessing a second blockchain that comprises one or more second blocks, wherein each of the one or more second blocks comprises

one or more access rights associated with one or more of the resources and/or one or more authorized users of the blockchain.

29. The method of claim 1, further comprising:

receiving an access request from a potential purchaser of the target building, wherein the access request comprises an indication of one or more resources stored on the blockchain for which access is sought;

determining one or more blocks of the blockchain that include at least a portion of the resources;

determining, based on the access policy, whether the potential purchaser is permitted to access the one or more resources; and

in response to determining that the potential purchaser is permitted to access the one or more resources, providing access to the one or more resources to the potential purchaser.

30. The method of claim 29, wherein:

the one or more resources correspond to one or more inspectors who conducted one or more inspections corresponding to the building rating system for the target building;

determining whether the potential purchaser is permitted to access the one or more resources comprises determining that the potential purchaser is permitted to access the one or more resources.

31. The method of claim 29, wherein:

the one or more resources correspond to one or more inspectors who did not conduct one or more inspections corresponding to the building rating system for the target building;

determining whether the potential purchaser is permitted to access the one or more resources comprises determining that the potential purchaser is not permitted to access the one or more resources.

32. The method of claim 29, further comprising accessing a second blockchain that comprises one or more second blocks, wherein each of the one or more second blocks comprises one or more access rights associated with one or more of the resources and/or one or more authorized users of the blockchain.

33. The method of claim 1, further comprising:

receiving an access request from the certification organization, wherein the access request comprises an indication of one or more resources stored on the blockchain for which access is sought;

determining one or more blocks of the blockchain that include at least a portion of the resources; and

determining, based on the access policy, whether the certification organization is permitted to access the one or more resources;

in response to determining that the certification organization is permitted to access the one or more resources, providing access to the one or more resources to the certification organization.

34. The method of claim 33, wherein:

the one or more resources correspond to one or more inspectors who conducted one or more inspections corresponding to the building rating system for the target building on behalf of the certification organization;

determining whether the certification organization is permitted to access the one or more resources comprises determining that the certification organization is permitted to access the one or more resources.

35. The method of claim 33, wherein:

the one or more resources correspond to one or more inspectors who did not conduct one or more inspections corresponding to the building rating system for the target building on behalf of the certification organization;

determining whether the certification organization is permitted to access the one or more resources comprises determining that the certification organization is not permitted to access the one or more resources.

36. The method of claim 33, further comprising accessing a second blockchain that comprises one or more second blocks, wherein each of the one or more second blocks comprises one or more access rights associated with one or more of the resources and/or one or more authorized users of the blockchain.

37. The method of claim 1, wherein:

the target blockchain further comprises a certification organization block comprising administration information associated with the building rating system that is administered by the certification organization, wherein the administration information includes one or more acceptable values and/or ranges of values associated with one or more tests that are performed as part of the building rating system,

the inspection information comprises one or more results of one or more of the tests,

the method further comprises determining whether the one or more results satisfy the one or more acceptable values and/or ranges of values,

in response to determining that the one or more results do not satisfy the one or more acceptable values and/or ranges of values:

automatically generating a notification of the inconsistency, and

sending the notification to the certification organization and/or the building owner.

38. The method of claim 1, further comprising:

generating a token for the building owner, wherein the token comprises:

an identifier associated with the building owner,

one or more of the one or more access rights that correspond to the building owner, and

for each of the one or more access rights that correspond to the building owner, an indication of a subset of information that is stored on the blockchain to which the access right corresponds; and

sending the token to the building owner.

39. The method of claim 38, wherein the token further comprises:

an indication of which of the access rights that correspond to the building owner the building owner can delegate to one or more business partners for each of the subsets of information that to which the access rights corresponds.

40. The method of claim 38, wherein the token further comprises an indication of how many tiers of delegation the building owner is permitted to make.

41. The method of claim 38, further comprising:

by an electronic device associated with the building owner:

generating a delegated token for a business partner that comprises:

an indication of one or more delegated access rights, wherein the delegated access rights comprise one or more of the access rights corresponding to the building owner, and

for each of the delegated access rights, an indication of at least a portion of the subset of information that is stored on the blockchain to which the delegated access rights correspond.

42. The method of claim 41, further comprising:

by the electronic device associated with the building owner:

generating a digital signature associated with the delegated token, and

sending the delegated token and the digital signature to the building owner.

43. The method of claim 42, wherein generating a digital signature associated with the delegated token comprises:

applying a hashing algorithm to at least a portion of the delegated token to yield a hashed value; and

encrypting the hashed value with a private key associated with the building owner.

44. The method of claim 1, further comprising:

generating a token for the identified certifier, wherein the token comprises:

an identifier associated with the identified certifier,

one or more of the one or more access rights that correspond to the identified certifier, and

for each of the one or more access rights that correspond to the identified certifier, an indication of a subset of information that is stored on the blockchain to which the access right corresponds; and

sending the token to the identified certifier.

45. The method of claim 44, wherein the token further comprises:

an indication of which of the access rights that correspond to the identified certifier the identified certifier can delegate to one or more business partners for each of the subsets of information that to which the access rights corresponds.

46. The method of claim 44, wherein the token further comprises an indication of how many tiers of delegation the identified certifier is permitted to make.

47. The method of claim 44, further comprising:

by an electronic device associated with the identified certifier:

generating a delegated token for a business partner that comprises:

an indication of one or more delegated access rights, wherein the delegated access rights comprise one or more of the access rights corresponding to the identified certifier, and

for each of the delegated access rights, an indication of at least a portion of the subset of information that is stored on the blockchain to which the delegated access rights correspond.

48. The method of claim 47, further comprising:

by the electronic device associated with the identified certifier:

generating a digital signature associated with the delegated token, and

sending the delegated token and the digital signature to the identified certifier.

49. The method of claim 48, wherein generating a digital signature associated with the delegated token comprises:

applying a hashing algorithm to at least a portion of the delegated token to yield a hashed value; and

encrypting the hashed value with a private key associated with the identified certifier.

50. The method of claim 1, further comprising:

generating a token for the identified inspector, wherein the token comprises:

an identifier associated with the identified inspector,

one or more of the one or more access rights that correspond to the identified inspector, and

for each of the one or more access rights corresponding to the identified inspector, an indication of a subset of information that is stored on the blockchain to which the corresponding access right corresponds; and

sending the token to the identified inspector.

51. The method of claim 50, wherein the token further comprises:

an indication of which of the access rights that correspond to the identified inspector the identified inspector can delegate to one or more business partners for each of the subsets of information that to which the access rights corresponds.

52. The method of claim 51, wherein the token further comprises an indication of how many tiers of delegation the identified inspector is permitted to make.

53. The method of claim 50, further comprising:

by an electronic device associated with the identified inspector:

generating a delegated token for a business partner that comprises:

an indication of one or more delegated access rights, wherein the delegated access rights comprise one or more of the corresponding access rights, and

for each of the delegated access rights, an indication of at least a portion of the subset of information that is stored on the blockchain to which the delegated access rights correspond.

54. The method of claim 53, further comprising:

by the electronic device associated with the identified inspector:

generating a digital signature associated with the delegated token, and

sending the delegated token and the digital signature to the identified inspector.

55. The method of claim 54, wherein generating a digital signature associated with the delegated token comprises:

applying a hashing algorithm to at least a portion of the delegated token to yield a hashed value; and

encrypting the hashed value with a private key associated with the identified inspector.

56. A system for securing data associated with one or more building rating systems, the system comprising:

one or more electronic devices; and

a computer-readable storage medium comprising one or more programming instructions that, when executed, cause one or more of the one or more electronic devices to perform the method of one or more of claims 1-55.

57. A computer program comprising one or more programming instructions that, when executed by one or more electronic devices, causes the one or more electronic devices to perform the method of one or more of claims 1-55.

58. A non-transitory computer-readable medium comprising one or more programming instructions that, when executed by one or more processors, performs the method of one or more of claims 1-55.

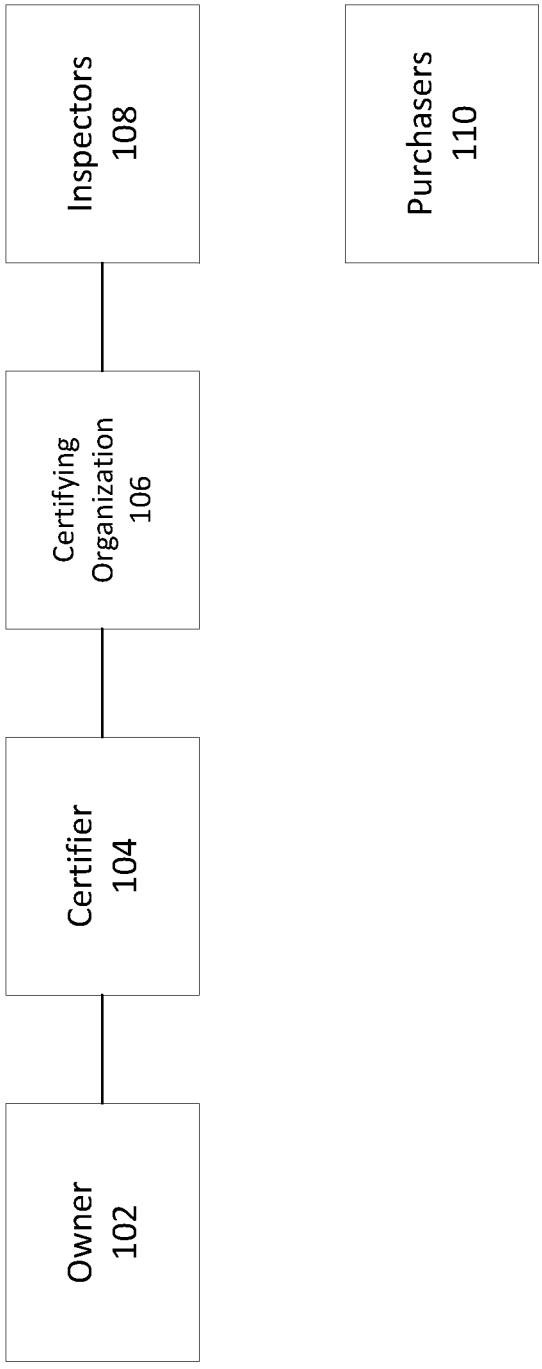
Inspectors
108
Purchasers
110
Certifying
Organization
106
Certifier
104
Owner
102

FIG. 1

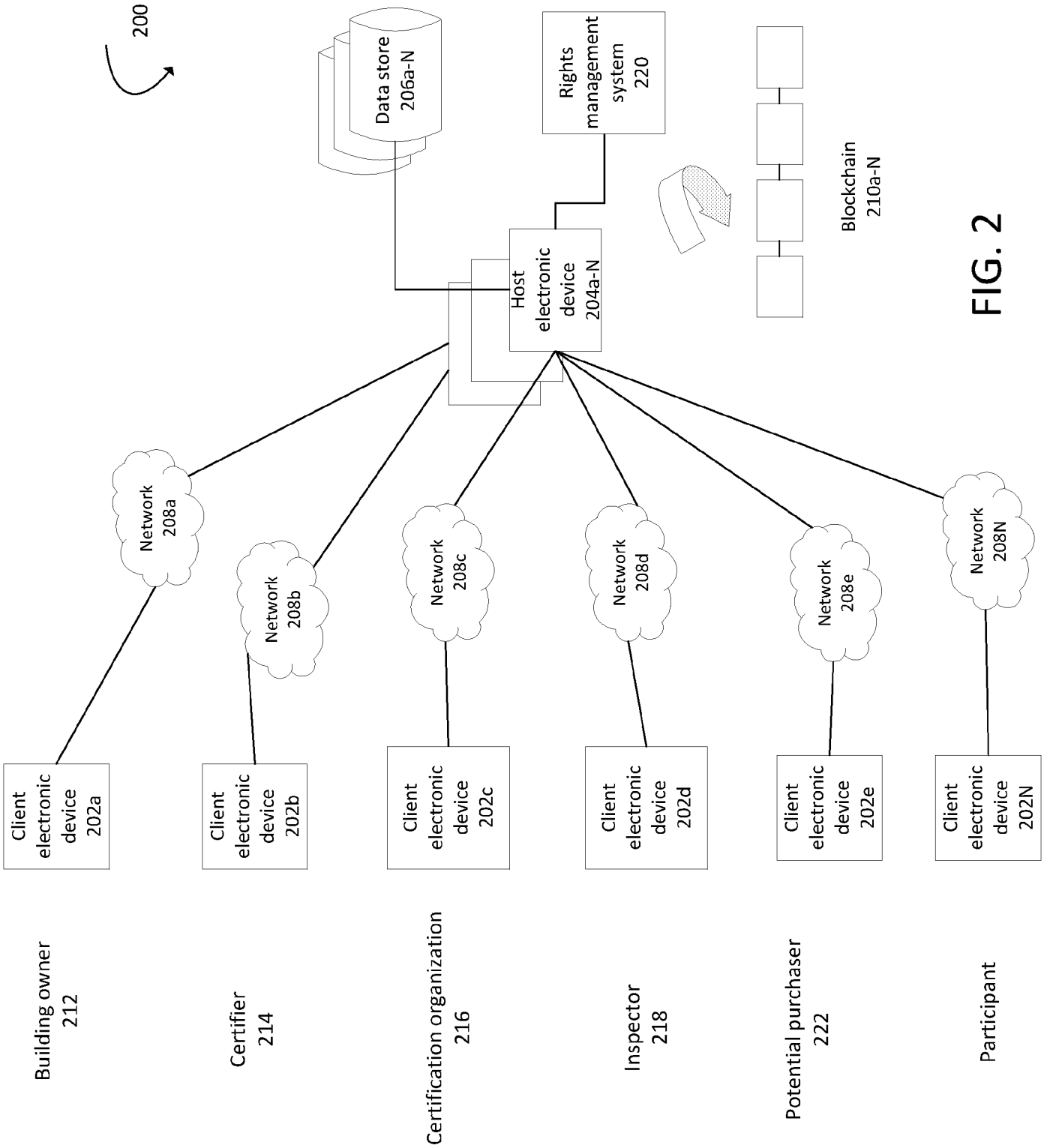
200
Data store 206a-N
Rights management system 220
Blockchain 210a-N
Host electronic device 204a-N
Network 208a
Network 208b
Network 208c
Network 208d
Network 208e
Network 208N
Client electronic device 202a
Client electronic device 202b
Client electronic device 202c
Client electronic device 202d
Client electronic device 202e
Client electronic device 202N
Building owner 212
Certifier 214
Certification organization 216
Inspector 218
Potential purchaser 222
Participant

FIG. 2

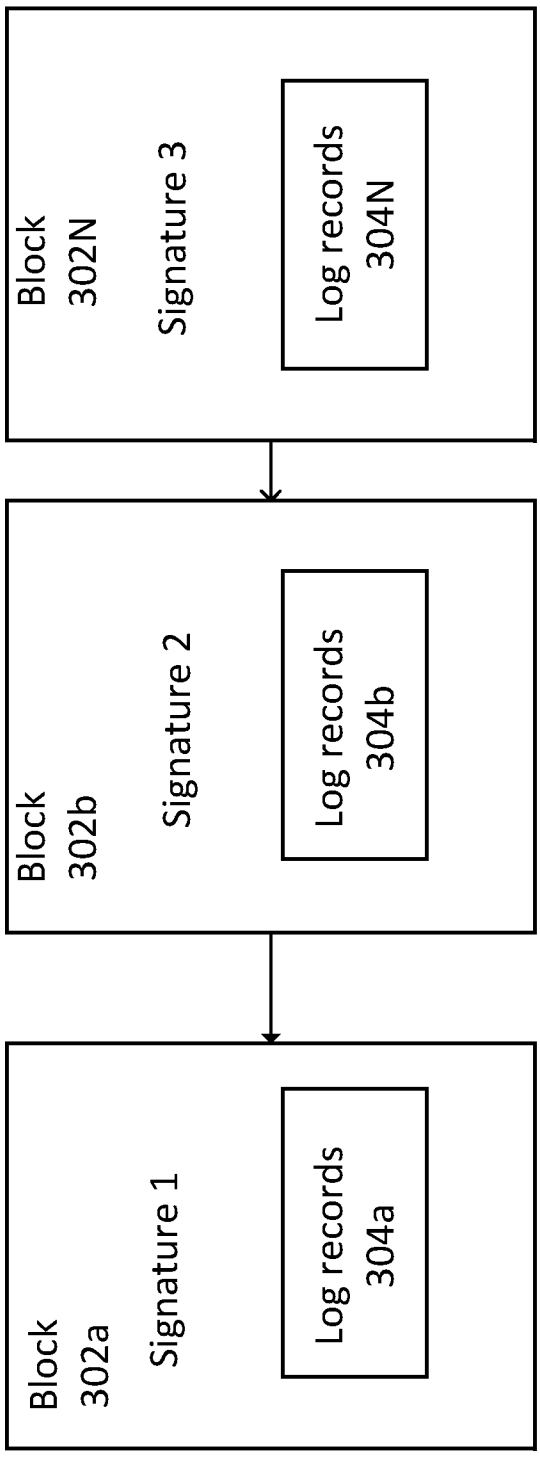
Block
302N
Signature 3
Log records
304N
Block
302b
Signature 2
Log records
304b
Block
302a
Signature 1
Log records
304a
Blockchain
300a-N

FIG. 3

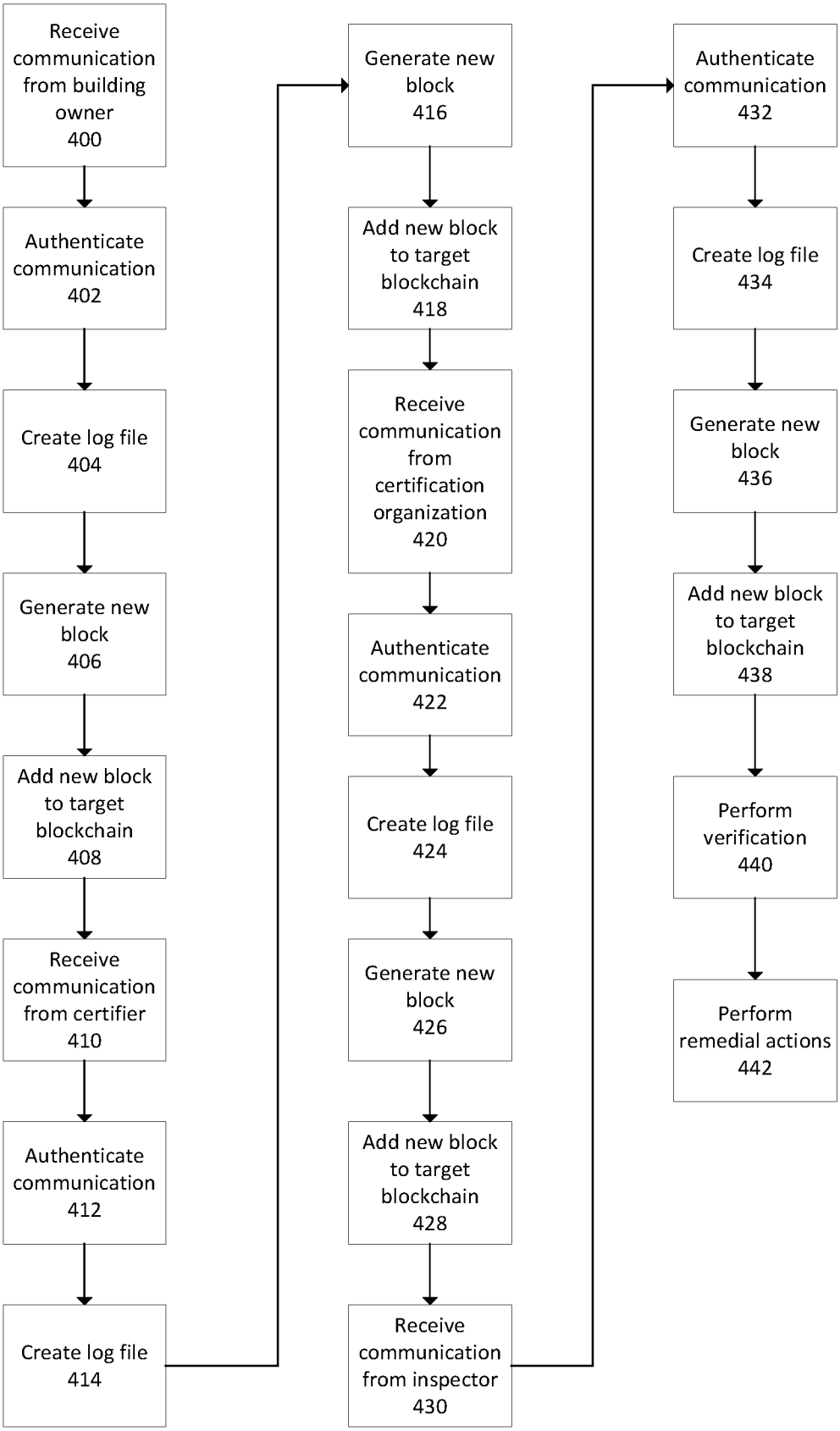
Receive communication from building owner 400
Authenticate communication 402
Create log file 404
Generate new block 406
Add new block to target blockchain 408
Receive communication from certifier 410
Authenticate communication 412
Create log file 414
Generate new block 416
Add new block to target blockchain 418
Receive communication from certification organization 420
Authenticate communication 422
Create log file 424
Generate new block 426
Add new block to target blockchain 428
Receive communication from inspector 430
Authenticate communication 432
Create log file 434
Generate new block 436
Add new block to target blockchain 438
Perform verification 440
Perform remedial actions 442

FIG. 4

Source identifier	Block identifier
Q2d3	Signature 1
G629	Signature 2
Q2d3	Signature 3
Ab63	Signature 4
Q2d3	Signature 5
G629	Signature 6
Ab63	Signature 7

FIG. 5

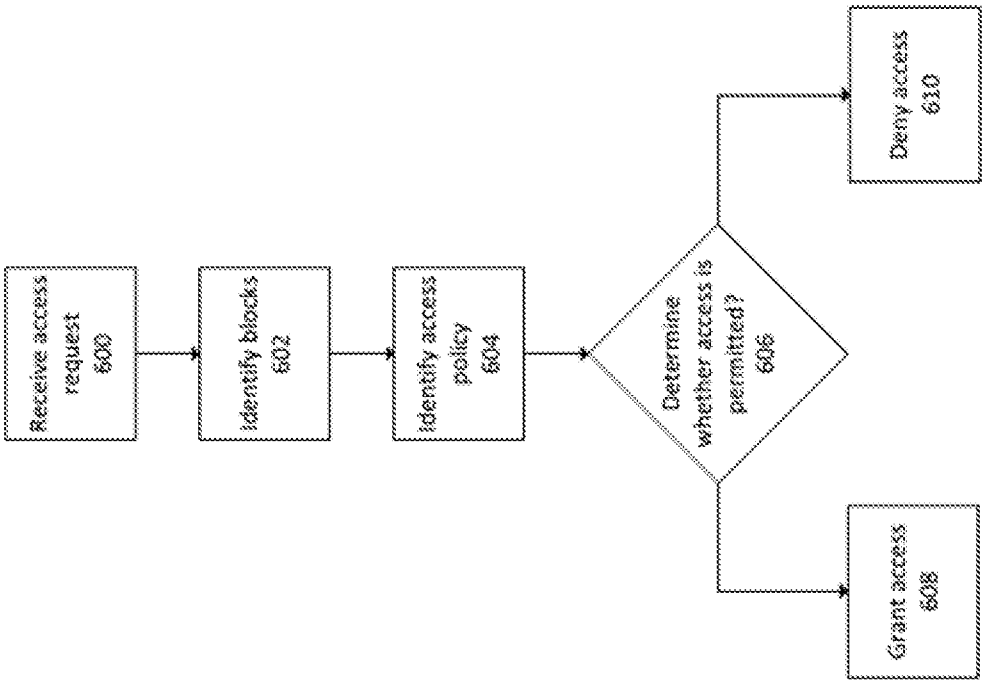
Receive access request 600
Identify blocks 602
Identify access policy 604
Determine whether access is permitted? 606
Deny access 610
Grant access 608

FIG. 6A

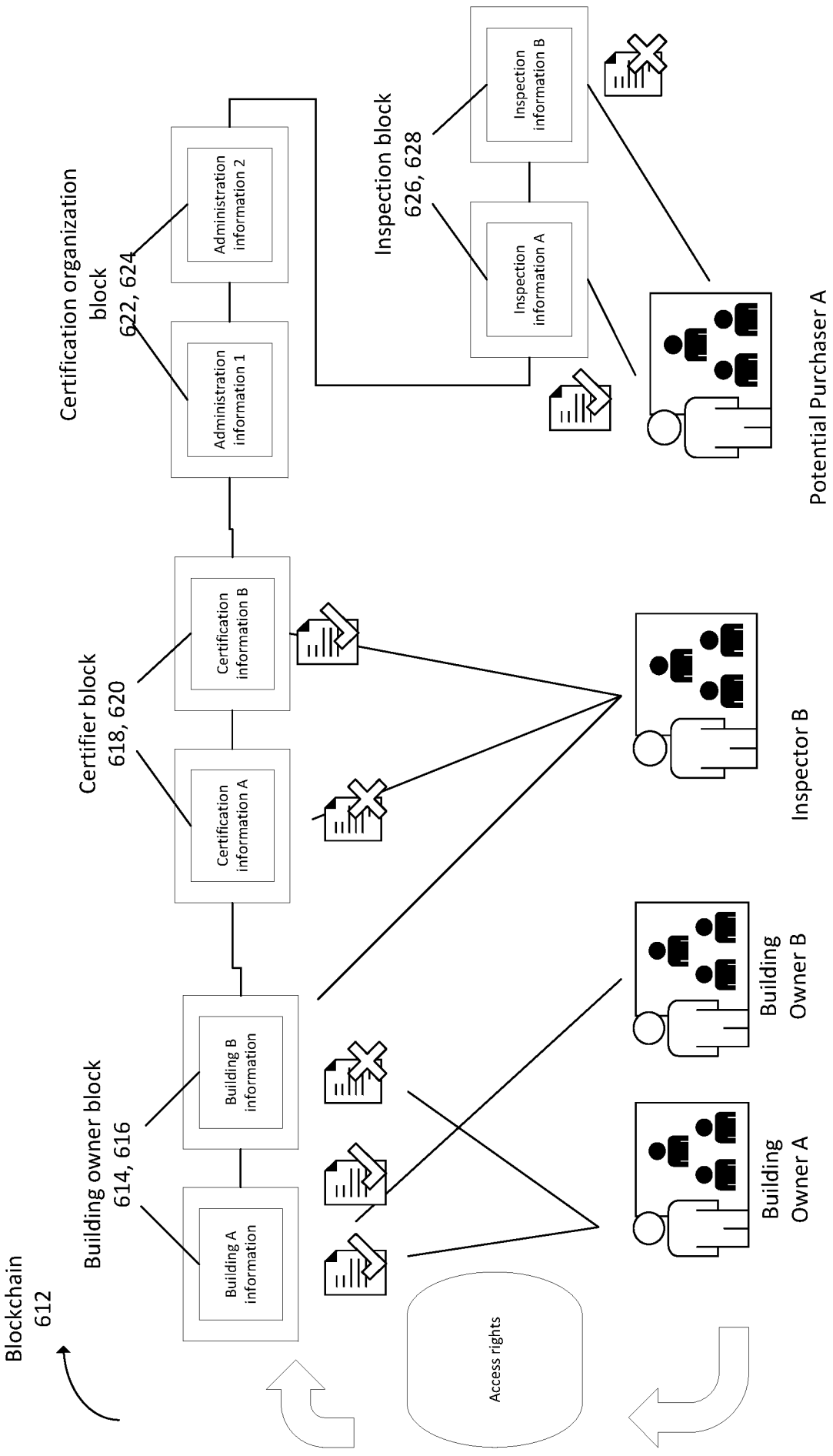
Blockchain
612
Building owner block
614, 616
Building A information
Building B information
Certifier block
618, 620
Certification information A
Certification information B
Certification organization block
622, 624
Administration information 1
Administration information 2
Inspection block
626, 628
Inspection information A
Inspection information B
Access rights
Building Owner A
Building Owner B
Inspector B
Potential Purchaser A

FIG. 6B

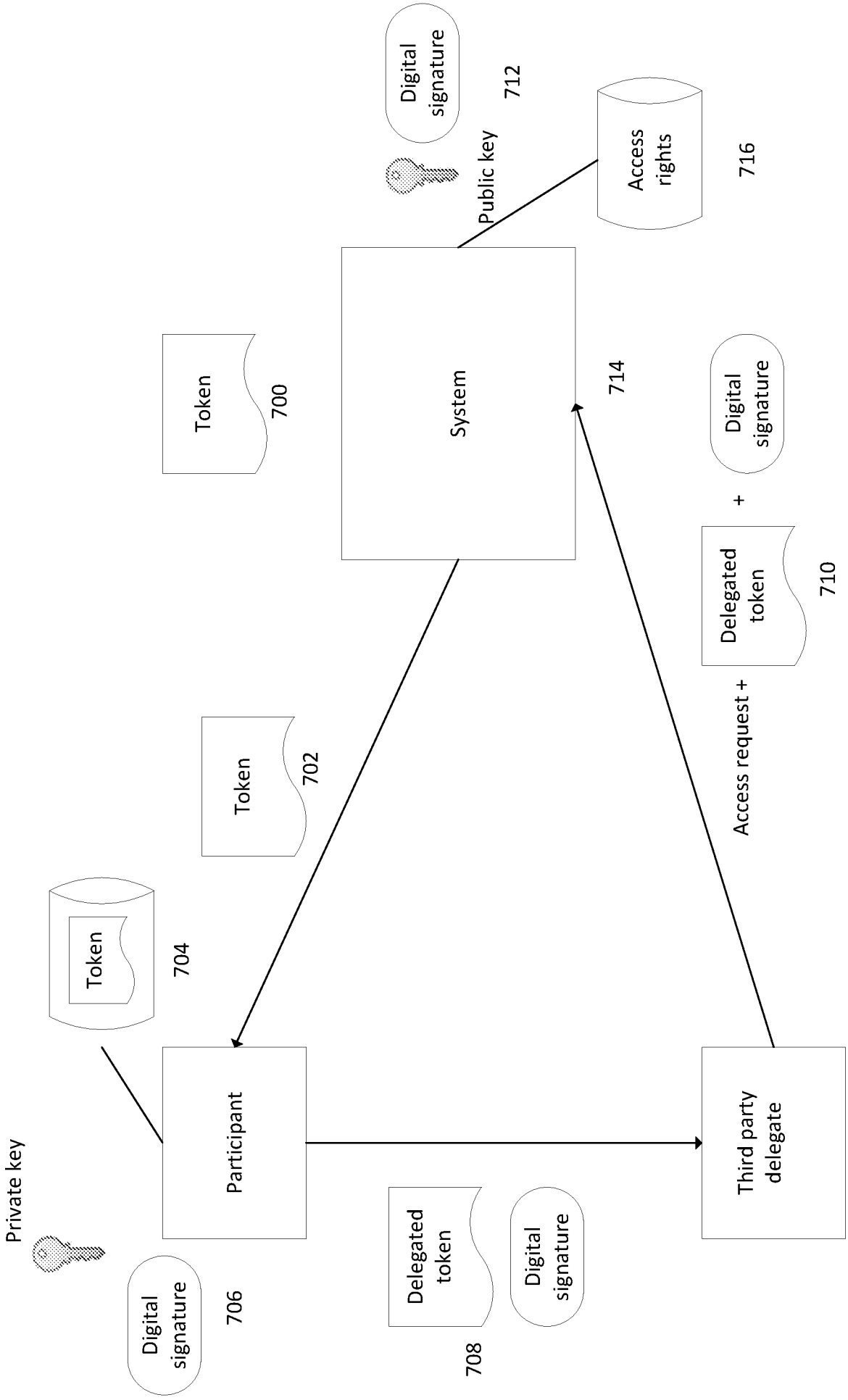
Digital signature
712
Public key
Access rights
716
Token
700
System
714
Digital signature
+
Delegated token
710
Token
702
Access request +
Token
704
Participant
Third party delegate
Private key
Digital signature
706
Delegated token
708
Digital signature

FIG. 7

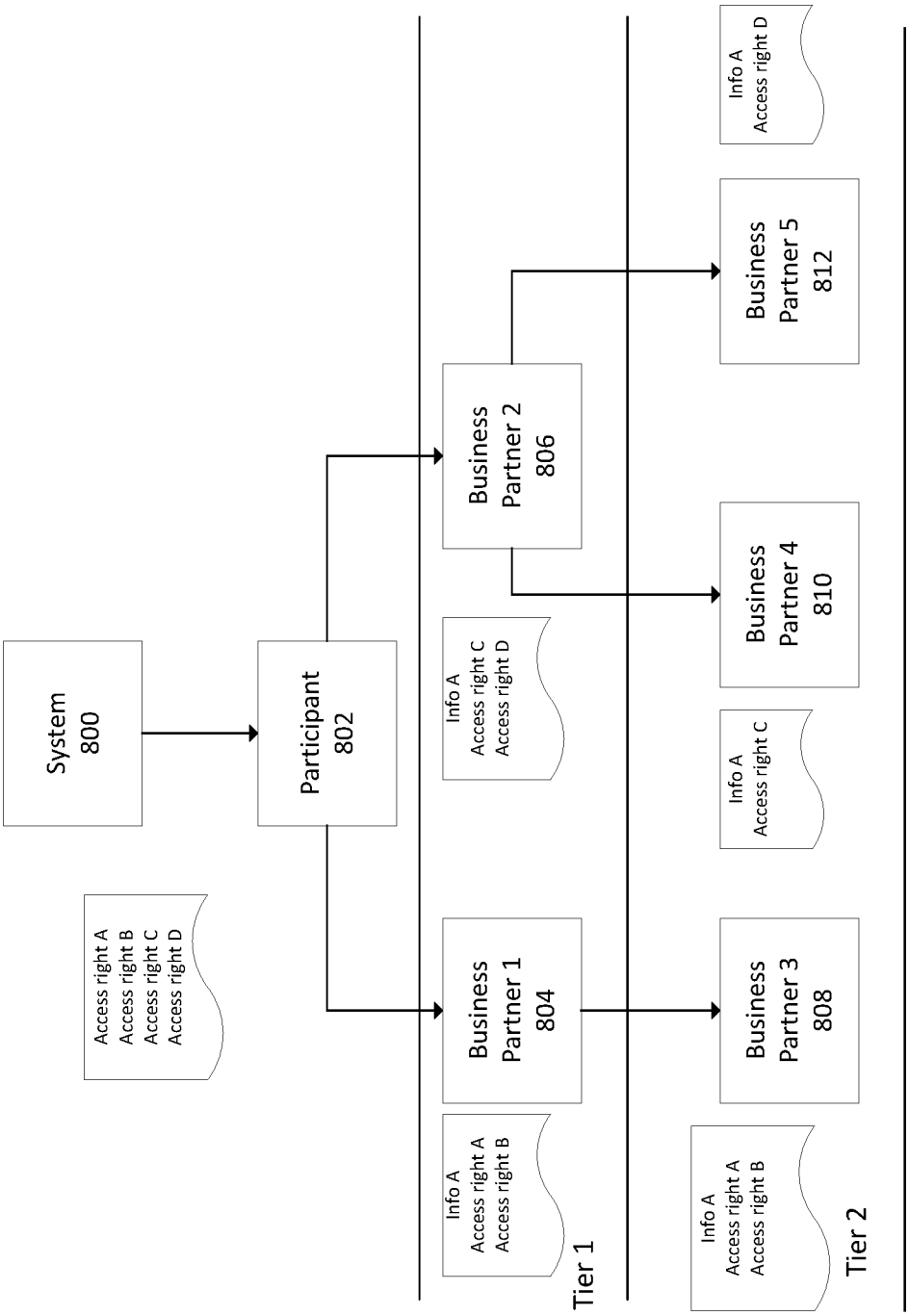
System
800
Participant
802
Access right A
Access right B
Access right C
Access right D
Business
Partner 1
804
Info A
Access right A
Access right B
Business
Partner 2
806
Info A
Access right C
Access right D
Business
Partner 3
808
Info A
Access right A
Access right B
Business
Partner 4
810
Info A
Access right C
Business
Partner 5
812
Info A
Access right D
Tier 1
Tier 2

FIG. 8

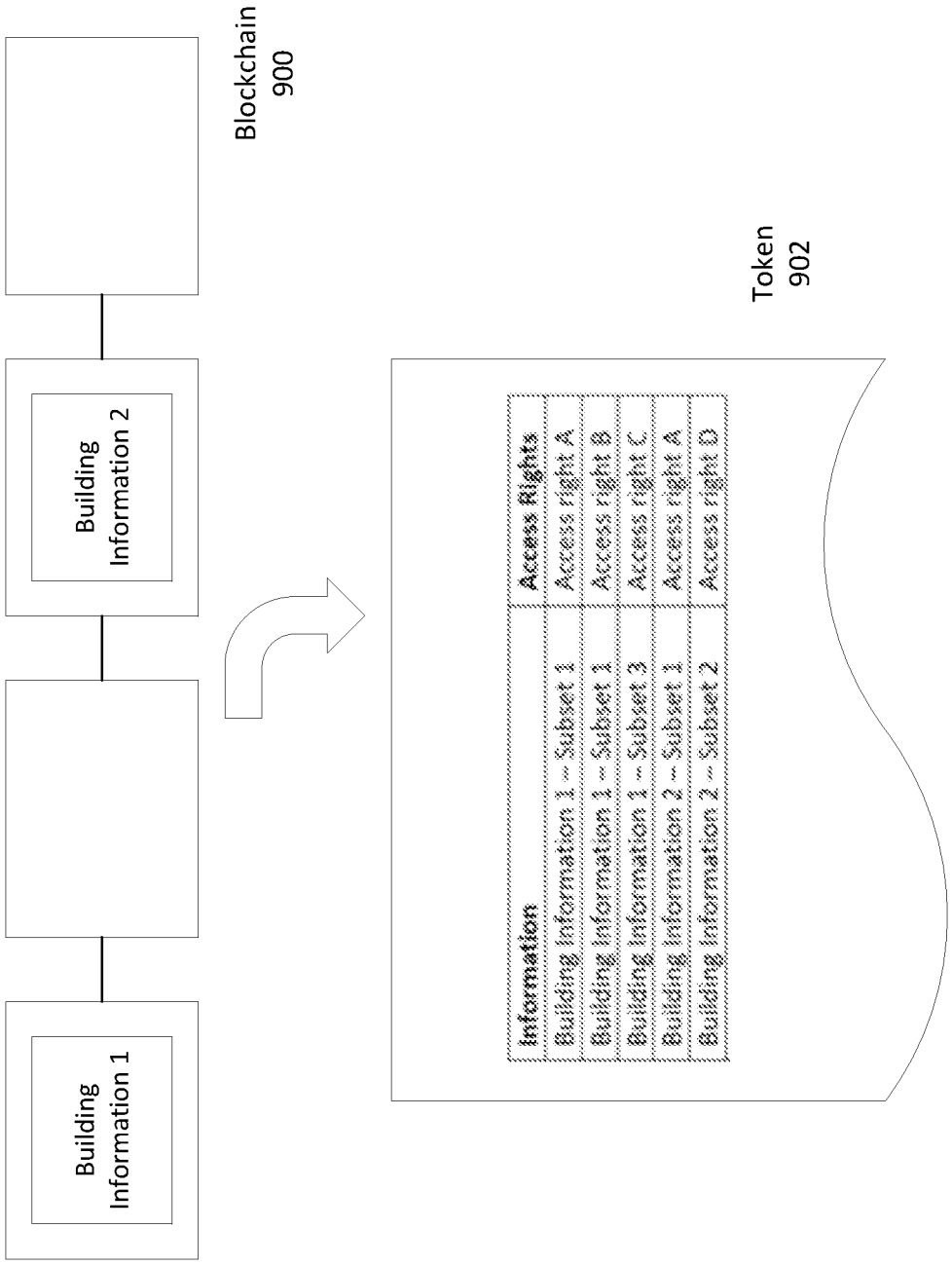
Building Information 1
Building Information 2
Blockchain 900
Token 902
Information
Access Rights
Building Information 1 – Subset 1
Access right A
Building Information 1 – Subset 1
Access right B
Building Information 1 – Subset 3
Access right C
Building Information 2 – Subset 1
Access right A
Building Information 2 – Subset 2
Access right D

FIG. 9A

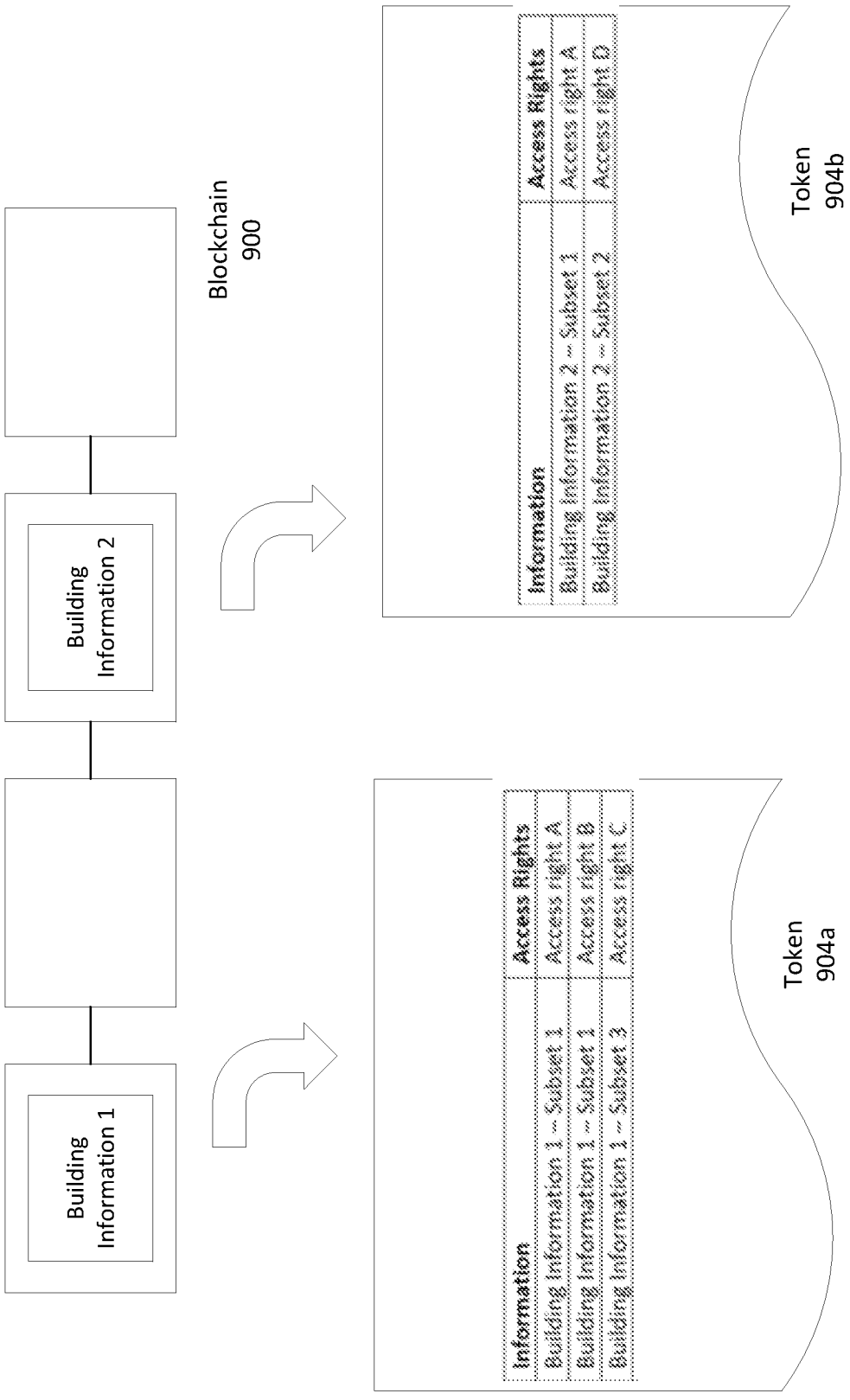
Building Information 1
Building Information 2
Blockchain 900
Information
Access Rights
Building Information 1 – Subset 1
Access right A
Building Information 1 – Subset 1
Access right B
Building Information 1 – Subset 3
Access right C
Token 904a
Information
Access Rights
Building Information 2 – Subset 1
Access right A
Building Information 2 – Subset 2
Access right D
Token 904b

FIG. 9B

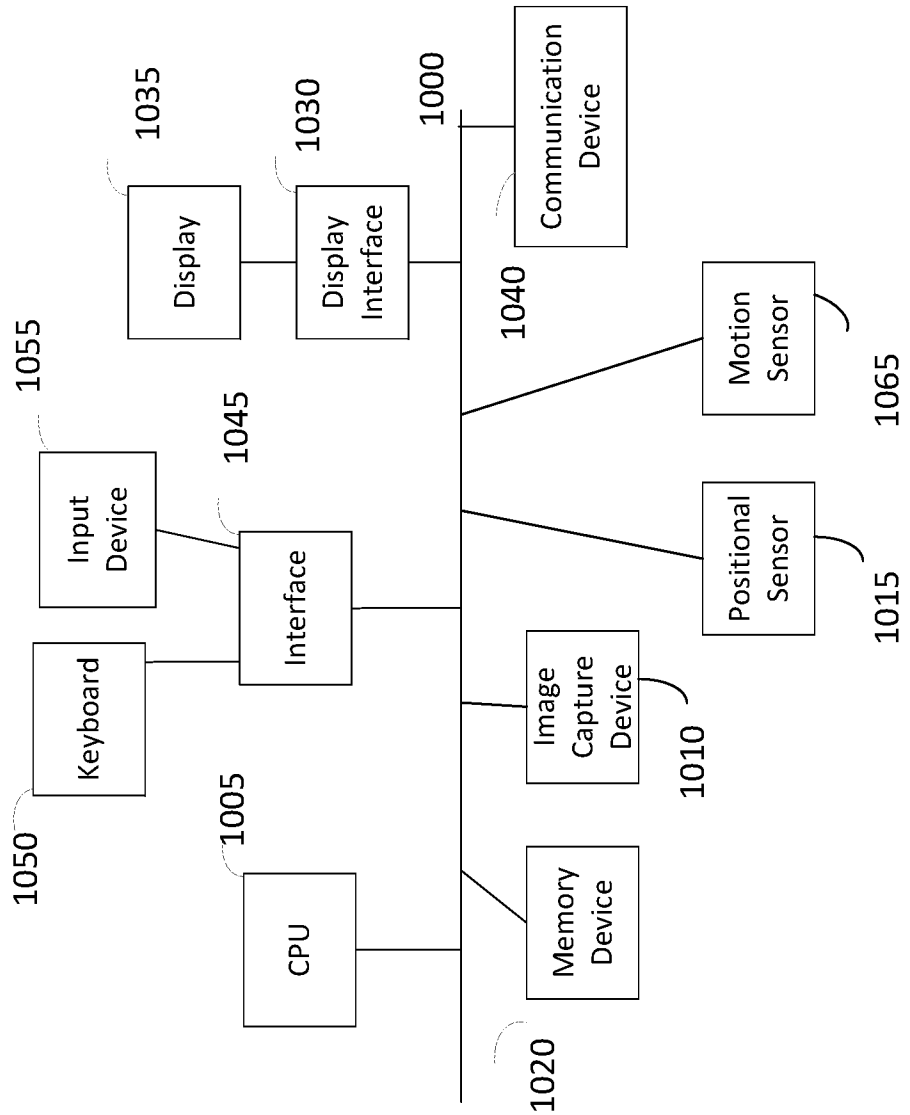
1000
1035
Display
1030
Display Interface
Communication Device
1040
1055
Input Device
1045
Interface
Motion Sensor
1065
Positional Sensor
1015
Keyboard
1050
1005
CPU
Image Capture Device
1010
Memory Device
1020

FIG. 10

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2022/029242

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q30/00
ADD.

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)
G06Q

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)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2020/302562 A1 (TRIM CRAIG M [US] ET AL) 24 September 2020 (2020-09-24) paragraph [0021] paragraph [0034] paragraph [0047] paragraph [0055] paragraph [0074] - paragraph [0075] figure 1	1-58
A	US 2020/052898 A1 (WENTZ CHRISTIAN T [US]) 13 February 2020 (2020-02-13) paragraph [0022] paragraph [0078]	2-8,15, 43,49,55

-/--

[x] Further documents are listed in the continuation of Box C.

[x] 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
9 September 2022	20/09/2022

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Stark, Konrad

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2022/029242

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2020/210978 A1 (BROWN SUZANNE [CH]) 2 July 2020 (2020-07-02) paragraph [0036] - paragraph [0037]	10,14, 38,41, 42,44, 47,48, 50,53,54

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2022/029242

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2020302562 A1	24-09-2020	NONE	
US 2020052898 A1	13-02-2020	NONE	
US 2020210978 A1	02-07-2020	US 2020210978 A1	02-07-2020
		WO 2020142504 A1	09-07-2020