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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 June 2020 (11.06.2020)

WIPO | PCT

(10) International Publication Number
WO 2020/118079 A1

(51) International Patent Classification:
G06F 21/35 (2013.01) *G07C 9/00* (2020.01)

(21) International Application Number:
PCT/US2019/064729

(22) International Filing Date:
05 December 2019 (05.12.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
201811487160.8 06 December 2018 (06.12.2018) CN

(71) Applicant: **CARRIER CORPORATION** [US/US]; 13995 Pasteur Blvd., Palm Beach Gardens, Florida 33418 (US).

(72) Inventors: **SHILA, Devu Manikantan**; 411 Silver Lane, East Hartford, Connecticut 06108 (US). **LARMUSEAU, Adriaan**; Room 3502, 35/F, Kerry Parkside Office, No. 1155 Fang Dian Road, Pudong New Area, Shanghai 201204 (CN). **KUENZI, Adam**; 4001 Fairview Industrial Dr. SE, Salem, Oregon 97302-1142 (US). **NOVOZHENETS, Yuri**; 1212 Pittsford - Victor Road, Pittsford, New York 14534 (US).

(74) Agent: **BURNS, David A.**; Cantor Colburn LLP, 20 Church Street, 22nd Floor, Hartford, Connecticut 06103-3207 (US).

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

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

(54) Title: BLOCKCHAIN SUPPORTED SMART LOCK SYSTEM

(57) Abstract: A system includes a processor, a storage medium, a data file, blockchain application, a lock assembly, and a digital key. The data file is stored in the storage medium, and is applied by the blockchain application. The data file includes a plurality of linked blocks, each including a respective transaction data of a plurality of transaction data. Each one of the plurality of transaction data includes a respective event and a time stamp. The blockchain application is stored in the storage medium, executed by the processor, and is configured to output an authorization based on a current grant event of a transaction data of the plurality of transaction data. The digital key is adapted to operate the lock assembly, wherein at least one of the lock assembly and the digital key is configured to receive the authorization in order for the digital key to operate the lock assembly.

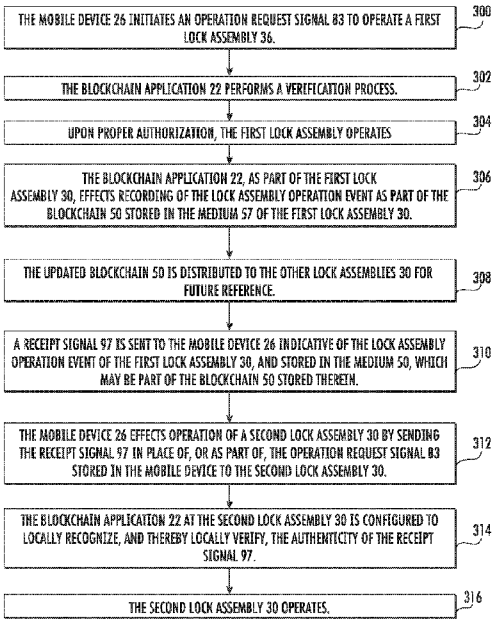

FIG. 7

WO 2020/118079 A1

[Continued on next page]

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

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

Published:

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

BLOCKCHAIN SUPPORTED SMART LOCK SYSTEM

BACKGROUND

[0001] The present disclosure relates to lock system, and more particularly, to a smart lock system supported by blockchain technology.

[0002] Smart lock systems may include one, or more smart locks, that may be managed by a central management system. Virtual, or digital, keys (i.e., keyless unlocking mechanisms) may be applied to operate specific locks as generally granted by the management and/or authentication system. Unfortunately, some smart lock applications require high security standards and confidence that the lock system is not being manipulated thereby placing any security, or historical records, in question.

BRIEF DESCRIPTION

[0003] A method of operating a smart lock system according to one, non-limiting, exemplary embodiment of the present disclosure includes sending a first operation request signal to a first lock assembly by a mobile device; performing a verification process by at least one blockchain application; upon verification, operating the first lock assembly; recording the operating of the first lock assembly as an operation event in a blockchain stored in a first storage medium of the first lock assembly; distributing the blockchain to a second storage medium of a second a second lock assembly; sending a receipt signal indicative of the occurrence of the operation event from the first lock assembly to the mobile device; sending a second operation request signal including information associated with the receipt signal by the mobile device and to a second lock assembly; recognizing the information associated with the receipt signal by the second lock assembly; and operating the second lock assembly.

[0004] In addition to the foregoing embodiment the second lock assembly includes a storage medium configured to store a blockchain application and the distributed blockchain, and the blockchain application is configured to utilize the distributed blockchain to effect operation of the second lock assembly.

[0005] A system according to another, non-limiting, embodiment includes at least one processor; at least one storage medium; a blockchain application stored in the at least one storage medium and executed by the at least one processor; a data file stored in the at least one storage medium and applied by the blockchain application, the data file including a plurality of linked blocks each including a respective transaction data of a plurality of transaction data, wherein each one of the plurality of transaction data includes a respective

event and a time stamp; a blockchain application stored in the at least one storage medium, executed by the at least one processor, and configured to output an authorization based on a current grant event of a transaction data of the plurality of transaction data; a lock assembly; and a digital key adapted to operate the lock assembly, wherein at least one of the lock assembly and the digital key is configured to receive the authorization in order for the digital key to operate the lock assembly.

[0006] In addition to the foregoing embodiment, the system comprises a server including a processor of the at least one processor and a storage medium of the at least one storage medium, wherein the block chain application is stored in the storage medium and executed by the processor.

[0007] In the alternative or additionally thereto, in the foregoing embodiment, the server is remote from the lock assembly.

[0008] In the alternative or additionally thereto, in the foregoing embodiment, the lock assembly includes a processor of the at least one processor and is configured to send a transaction data signal indicative of an event and to the processor of the server toward growth of the plurality of the plurality of linked blocks.

[0009] In the alternative or additionally thereto, in the foregoing embodiment, the digital key is a key application loaded into a smart phone.

[0010] In the alternative or additionally thereto, in the foregoing embodiment, the digital key is a key application loaded into a smart phone, and the smart phone is configured to wirelessly send an access command to the lock assembly.

[0011] In the alternative or additionally thereto, in the foregoing embodiment, the plurality of transaction data includes a grant transaction data including a grant event, a key address, a lock address, and a time stamp.

[0012] In the alternative or additionally thereto, in the foregoing embodiment, the plurality of transaction data includes an unlock transaction data including an unlock event, a key address, a lock address, and a time stamp.

[0013] In the alternative or additionally thereto, in the foregoing embodiment, the plurality of transaction data includes an unlock transaction data including an unlock event, a key address, a lock address, and a time stamp.

[0014] In the alternative or additionally thereto, in the foregoing embodiment, the plurality of transaction data includes a lock transaction data including a lock even, a lock address, and a time stamp.

[0015] In the alternative or additionally thereto, in the foregoing embodiment, the plurality of transaction data includes a lock transaction data including a lock even, a lock address, and a time stamp.

[0016] In the alternative or additionally thereto, in the foregoing embodiment, the plurality of transaction data includes an access deny transaction data including an access deny event, a key address, a lock address, and a time stamp.

[0017] A method of operating a lock system according to another, non-limiting, embodiment, includes applying a digital key to a lock assembly to effect an unlock event; sending an authorization request communication by the lock assembly to a control arrangement; applying a blockchain application by the control arrangement to verify the authorization request; sending an access verification to the lock assembly; unlocking the lock assembly; sending an unlock event signal to the blockchain application, wherein the unlock event signal includes an unlock event, a lock assembly address, and a key address; creating unlock transaction data indicative of the unlock event signal by the blockchain application; and configuring the unlock transaction data as a block of a plurality of linked blocks and applying a time stamp by the blockchain application.

[0018] The foregoing features and elements may be combined in various combinations without exclusivity, unless expressly indicated otherwise. These features and elements as well as the operation thereof will become more apparent in light of the following description and the accompanying drawings. However, it should be understood that the following description and drawings are intended to be exemplary in nature and non-limiting.

BRIEF DESCRIPTION OF THE DRAWINGS

[0019] Various features will become apparent to those skilled in the art from the following detailed description of the disclosed non-limiting embodiments. The drawings that accompany the detailed description can be briefly described as follows:

[0020] FIG. 1 is a schematic of a system as one, non-limiting, exemplary embodiment of the present disclosure;

[0021] FIG. 2 is a schematic of a digital key of the system;

[0022] FIG. 3 is a schematic of a lock assembly of the system;

[0023] FIG. 4 is a schematic of a data file used by a blockchain application of the system;

[0024] FIG. 5 is a flow chart illustrating a method of operating the system;

[0025] FIG. 6 is a flow chart illustrating a method of verifying a user of the system; and

[0026] FIG. 7 is a flow chart illustrating another method of operating the system.

DETAILED DESCRIPTION

[0027] Referring to FIG. 1, a system 20 (e.g., smart lock system) may include, and is supported by, a blockchain application 22 to enhance security and provide historical records (i.e., transactions) with a high degree of confidence. The system 20 may include a control arrangement 24, a plurality of digital, or virtual, keys 26 that may be carried by respective human beings 28, and a plurality of smart lock assemblies 30. The term "smart" in smart lock assemblies refer to an electronic device that may generally be connected to other devices or networks via various wireless protocols such as Bluetooth, NFC, Wi-Fi, LiFi, 3G and others. The smart lock assemblies 30 may also operate, to a degree, interactively and autonomously. Examples of the digital key 26, may be an access card with a magnetic strip, a smart phone with a preloaded lock application, tablets, smart bands, and others. Applications of use regarding the smart lock assemblies 28 may be human access doors (e.g., hotel room doors), vaults, safes, mailboxes, keyboxes, padlocks, Bluetooth modules, and others.

[0028] The control arrangement 24 may include a server 32 and an administrative or management controller 34 that may be local (e.g., located within a hotel wherein the lock assemblies 30 are an integral part of hotel room doors). The server 32 may be run remotely or locally, and/or may be cloud or web based. In one example, the server 32 may not be in direct communication with the local controller 34. It is further contemplated and understood that the controller 34 may be an integral part of the server 32 (i.e., may share the same processor and computer readable storage medium).

[0029] The remote server 32 may include an electronic processor 36 (e.g., microprocessor), an electronic storage medium 38 that may be computer readable and writeable, and a transceiver 40 for wireless communications. In one embodiment, the blockchain application 22 may be stored in the storage medium 38 and, at least in-part, executed by the processor 36 of the server 32. The controller 34 may include a computing processor 42 (e.g., microprocessor), an electronic storage medium 44 that may be computer readable and writeable, and in some applications, a transceiver 46 for wireless communications. Referring to FIG. 2, each one of the digital keys 26 may include an electronic processor 48 (e.g., microprocessor), an electronic storage medium 50 that may be

computer readable and writeable, a user interface 49, and a transceiver 54 for wireless communications.

[0030] Referring to FIG. 3, the lock assembly 30 may be smart, and may include an electronic processor 55 (e.g., microprocessor), an electronic storage medium 57 that may be computer readable and writeable, a transceiver 59 for wireless communications, and a latch or lock mechanism 61. In one embodiment, the transceiver 59 is configured to receive signal(s) from the digital key 26 (e.g., mobile device) and transmit signals to the controller 34 and/or the server 32.

[0031] The term "blockchain" refers to a list of records (i.e., called blocks) capable of growth, and linked using cryptography. Each block may contain a cryptographic hash of the previous block, a timestamp, and transaction data. By design, blockchains are resistant to modification of the transaction data, and is generally an open distributed ledger that can record transactions between parties, and/or entities, efficiently and in a verifiable and permanent way. When applied as a distributed ledger, the blockchain may be managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be changed retroactively without a change to all subsequent blocks. Such a change to all subsequent blocks may require a consensus of the network majority.

[0032] Referring to FIG. 4, the storage medium 38 of the server 32 may also store a plurality of linked blocks 50 (i.e., the blockchain) as part of a data file 51 accessible and applied by the blockchain application 22. Each block 50 includes one of a variety of transaction data types. For example, grant or asset transaction data 52 (i.e., grant authorization) includes grant event 54 to a specific digital key 26 with regard to at least one lock assembly 30, a key or device address 56 indicative of the specific digital key 26, a lock address 58 indicative of the specific lock assembly 30, and a time stamp 60. The transaction data 52 may further include the name and personal information of the human being 28 assigned to the digital key 26.

[0033] In another embodiment, the grant transaction data 52 may include an identity that refers to the human being 28 assigned the digital key 26. In this embodiment, if the device address 56 matches the digital key 26, then the human being 28 may gain access.

[0034] In yet another embodiment, the digital key 26 may be a mobile device (e.g., smart phone), and may be configured to declare an identity to the lock assembly 30 (i.e., "I am identity xyz"). The blockchain application 22 may then search for recorded access right to "xyz" as part of the blockchain 50. In order to prove that this is really the person who is

identified by "xyz," the lock assembly 30 may contact a service and verify the identity, or the mobile device 26 would verify the identity and certify the identity to the lock assembly 30. The lock assembly 30 may then verify the certificate. In all techniques, something is recorded on the blockchain 50 that the blockchain application 22 may check at the request of the lock assembly 30 to confirm access rights.

[0035] An unlock transaction data 62 may include an opening, or unlock, event 64 of a specific lock assembly 30, the specific lock address 58, the specific key address 56, and a time stamp 66 of the opening event 64. Locking transaction data 68 may include a closing, or locking, event 70 of the specific lock assembly 30, the specific lock address 58, and a time stamp 72 of the locking event 70. With regard to transaction data 68, the locking event 70 may occur automatically without use of a digital key 26. For example, a hotel room door that incorporates a lock assembly 30 may be biased toward a closed position, and once the door closes, the lock assembly 30 may be adapted to automatically lock.

[0036] In another example of a transaction data type, denied transaction data 74 includes an access deny event 76 to a specific lock assembly 30 utilizing a specific digital key 26, the key address 56 indicative of the specific digital key 26, the lock address 58 indicative of the specific lock assembly 30, and a time stamp 78. The transaction data 74 may further include the name and personal information of the human being 28 denied access via the digital key 26.

[0037] In yet another example, access removed transaction data 78 may include an access removal event 80, wherein a human being 28 (or the digital key 26 carried by the human being) is denied access to, or the ability to unlock, a specific lock assembly 30. The transaction data 78 may further include a key address 82, a lock address 84, and a time stamp 86. In one example, the key address 82 may be a wireless device address that generally transmits the digital key signal.

[0038] Referring to FIGS. 1-4, and in operation, an administrator at the local controller 34 of the control arrangement 24 may initiate an access grant signal 81 with regard to a specific key 26 and specific lock assembly 30. The access grant signal 81 may be received by the blockchain application 22. The application 22 may then create and link a block 50 indicative of the grant transaction data 52. With this grant authorization, the specific key 26 may now operate the specific lock assembly 30. In one embodiment, the access grant is not pre-stored by the lock assembly 30 and/or the key 26. Instead, the grant is stored as part of the data file 51 and is referred to by the lock assembly 30 and/or the key 26 upon initiation of the next transaction (e.g., an unlock event).

[0039] When the key 26 attempts to unlock the lock assembly 30 (see arrow 83 indicative of an actuation request signal or reading from the key), the lock assembly 30 may send an authorization request signal (see arrow 85) to the server 32. In one example, signal 85 may be sent from the lock assembly 30 via a network, and to the cloud server 332. The blockchain application 22 may then refer to the data file 51 to determine if the current block 50, or current relative block, confirms access grant (i.e., the grant transaction data 52). If yes, the blockchain application 22 effects an output by the server 32 as an access verification signal (see arrow 87) to the requesting lock assembly 30. Once received, the lock assembly 30 may reposition to an unlock state.

[0040] Referring to FIG. 5, a method of operating the system 20 is illustrated. At block 100, a digital key 26 is applied to a lock assembly 30 to effect an unlock event 64. At block 102 an authorization request communication, or signal, 85 is sent by the lock assembly 30 to the control arrangement 24. At block 104, the control arrangement 24 applies the blockchain application 22 to verify the authorization request. At block 106, the control arrangement 24 sends an access verification signal 87 to the lock assembly 30. At block 108, the lock assembly 30 unlocks.

[0041] At block 110, and after the lock assembly 30 unlocks, the lock assembly 30 may send an unlock event signal (see arrow 88 in FIG. 1) to the blockchain application 22. The unlock event signal 88 may include information pertaining to the unlock event, the associated lock address, and the associated key address. At block 112, the blockchain application 22 may then create unlock transaction data indicative of the unlock event signal. At block 114, the blockchain application 22 configures the unlock transaction data as a block of a plurality of blocks 50, and applies a time stamp to the block.

[0042] In another embodiment, the system 20 may be a transferable realestate asset system (i.e., an assignable realestate system) applied to realestate 90 (see FIG. 1). The realestate 90 may be hotel rooms, residential homes, and other dwellings. In this embodiment, the digital key 26 (see FIG. 2) is a mobile wireless device configured to wirelessly transmit an actuation request signal 83 that is generally a digital key signal or the digital key itself. The signal 83 may contain a wireless device address 92 preprogrammed and stored in the storage medium 49 along with a preprogrammed key application 93 executed by the processor 48 of the device 26 to generate the request signal 83.

[0043] In the present disclosure, the digital key, or signal 83, is not generally defined by a secretive sequence of bytes. Instead, the signal 83 is defined by the account that owns it (i.e., the wireless device address 92). This ownership of the digital key is determined through

a distributed ledger of verified transactions that constitute a blockchain (i.e., the plurality of linked blocks 50).

[0044] As previously described, at least a portion of the plurality of linked blocks 50 may respectively contain a plurality of different asset transaction data 52 each with a different time stamp. The most current asset transaction data 52 is the effective or appropriate asset transaction data 52, and the only data capable of transferring the asset (i.e., realestate 90). More specifically, the human being 28 carrying and operating the mobile wireless device 26 associated with the current asset transaction data 52 is the only human being 28 accredited with the right to open a door 91 utilizing the lock assembly 30 (see FIG. 1). Any other asset transaction data contained in other blocks 52 with preceding time stamps is not the most current. That is, a different user of a different mobile device with a different address, and with a preceding time stamp, is not accredited access.

[0045] In one embodiment, the current asset transaction data 52 may be generated by an administrator from the administrative controller 34. An assignment application 94 may be stored in the storage medium 44 of the controller 34 and executed by the processor 42. The assignment application 94 receives authorization commands (see arrow 95) from the administrator. The command 95 may include the address 56 of the mobile device 26 and instructions to grant access. The application 94 may then effect the transmission, via transceiver 46, of the grant access signal 81 to the blockchain application 22 for development of the current asset transaction data 52.

[0046] Referring to FIG. 6 and in operation of the transferrable realestate asset system 20, and at block 200, a human being 28 may effect the transmission of an actuate request signal 83 from a transceiver 54 of a wireless device 26 carried by a human being 28. At block 202, the transceiver 59 of the lock assembly 30 receives signal 83, then the processor 55 processes the signal 83 and generates an authorization request signal 85. The transceiver 59 transmits the signal 85 to server 32. If the server 32 is a cloud server, transmission of signal 85 may be facilitated by a network.

[0047] At block 204, the transceiver 40 of the server 32 receives the authorization request signal 85, the processor 36 processes the signal utilizing the blockchain application 22 and the data file 51. At block 206, the blockchain application 22 determines the current asset transaction data 52. At block 208 and if the device address 56 recorded as part of the current asset transaction data 52 of a block 50 correlates with signal 85, the blockchain application 22 determines that the human being 28 of the device 26 should be accredited the asset, and thus access should be granted through the door 91 via actuation of the lock

assembly 30. To accomplish this, and at block 210, the processor 36 of the server 32 sends a verification signal 87 via the transceiver 40 to the lock assembly 30. At block 212, the processor 55 processes the signal 87 and instructs the lock mechanism 61 to, for example, unlock the door 91. This ability of a human being 28 with the current, or verified, device 26, to unlock the door 91 is the symbolic transference of realestate 90 associated with the access door 91.

[0048] The strong verification properties of the blockchain ensure the human being 28 with the current mobile device 26 is the only one able to access the realestate at the current time. In addition to implementing smart lock access as blockchain based assets, the assets may now be governed by smart contracts that can securely automate common realestate or hotel transactions. Smart contracts can trade the ownership of houses between realtors or hotel rooms between guests without any direct interaction between the involved parties. In addition, all lock transactions are stored on the blockchain in a manner that cannot be altered retroactively or forged. Such secure and unalterable smart lock transaction logging can be used to prove the financial value of the house or hotel room.

[0049] Referring to FIG. 7, another embodiment of a method of operating the system 20 is illustrated. As part of this method, at least a portion of the blockchain application 22 and the blockchain 50 is stored in the mediums 57 of each lock assembly 30 and executed by the respective processors 55 (i.e., the distributed ledger). At least a portion of the application 22 and the blockchain 50 may further be stored and executed in the medium 50 and processor 48 of each mobile device 26, and stored and executed in the respective medium 44 and processor 42 of the controller 34. In this embodiment, the blockchain 50 may be distributed directly between lock assemblies 30 as a signal (see arrows 96 in FIG. 1). In this embodiment, the system 20 is configured to reduce the latency associated with operating a lock assembly 30 by delegating "trust" from one lock assembly 30 to another. The blockchain signal 96 may be sent over wireless pathways via the transceivers 46, or may be sent over hard wired pathways.

[0050] At block 300, the mobile device 26 carried by, and associated with, a human being 28 initiates an operation request signal 83 to operate (e.g., unlock) a first lock assembly 36. At block 302, the blockchain application 22 performs a verification process. This verification process may include the authorization request signal 85 as previous described. At block 304 and upon proper authorization, the first lock assembly 30 operates (e.g., unlocks) per the request of the mobile device 26. At block 306, the blockchain application 22, as part of the first lock assembly 30, effects recording of this operation event as part of

the blockchain 50 stored in the medium 57 of the first lock assembly 30. At block 308, the updated blockchain 50 may be distributed to the other lock assemblies 30 for future reference. At block 310, a receipt signal (see arrow 97 in FIG. 1) is sent to the mobile device 26 indicative of the operating event of the first lock assembly 30, and stored in the medium 50, which may be part of the blockchain 50 stored therein.

[0051] At block 312, the human being 28 with the same mobile device 26 of block 300, utilizes the mobile device 26 to operate a second lock assembly 30 by sending the receipt signal 97 in place of, or as part of, the operation request signal 83 stored in the mobile device to the second lock assembly 30 (see FIG. 1). At block 314, the blockchain application 22 at the second lock assembly 30 is configured to locally recognize, and thereby locally verify, the authenticity of the receipt signal 97. At block 316, the second lock assembly 30 operates (e.g. unlocks). In this way, faster verification to unlock the second lock assembly 30 is achieved, on the belief that the human being 28 has authenticated to the first lock assembly 30 successfully, and therefore does not require the presentation of the whole set of credentials a second time (i.e., the verification process). To unlock the second lock assembly 30, only a minimal set of credentials (i.e., the receipt signal 97) is exchanged with the second lock assembly 30, in order to reduce communication latency. This is the meaning of "delegated trust." The blockchain 50 is a record of all operations to ensure trustworthy operations.

[0052] Advantages and benefits of the present disclosure include a blockchain based distributed ledger for smart lock systems that provides a verified time stamped authentication receipts, ensuring customers have a high degree of confidence in the security of the system. Other advantages include a digital key that is not easily shared between users through malicious means, or counterfeiting.

[0053] The various functions described above may be implemented or supported by a computer program that is formed from computer readable program codes, and that is embodied in a computer readable medium. Computer readable program codes may include source codes, object codes, executable codes, and others. Computer readable mediums may be any type of media capable of being accessed by a computer, and may include non-transitory mediums, Read Only Memory (ROM), Random Access Memory (RAM), a hard disk drive, a compact disc (CD), a digital video disc (DVD), or other forms.

[0054] Terms used herein such as component, application, module, system, and the like are intended to refer to a computer-related entity, either hardware, a combination of hardware and software, or software execution. By way of example, an application may be, but is not limited to, a process running on a processor, a processor, an object, an executable, a

thread of execution, a program, a software instruction, and/or a computer. It is understood that an application running on a server and the server, may be a component or arrangement. One or more applications may reside within a process and/or thread of execution and an application may be localized on one computer and/or distributed between two or more computers.

[0055] While the present disclosure is described with reference to illustrated embodiments, it will be understood by those skilled in the art that various changes may be made and equivalents may be substituted without departing from the spirit and scope of the present disclosure. In addition, various modifications may be applied to adapt the teachings of the present disclosure to particular situations, applications, and/or materials, without departing from the essential scope thereof. The present disclosure is thus not limited to the particular examples disclosed herein, but includes all embodiments falling within the scope of the appended claims.

What is claimed is:

1. A method of operating a smart lock system comprising:

sending a first operation request signal to a first lock assembly by a mobile device;

performing a verification process by at least one blockchain application;

upon verification, operating the first lock assembly;

recording the operating of the first lock assembly as an operation event in a blockchain stored in a first storage medium of the first lock assembly;

distributing the blockchain to a second storage medium of a second a second lock assembly;

sending a receipt signal indicative of the occurrence of the operation event from the first lock assembly to the mobile device;

sending a second operation request signal including information associated with the receipt signal by the mobile device and to a second lock assembly;

recognizing the information associated with the receipt signal by the second lock assembly; and

operating the second lock assembly.

2. The method set forth in claim 1, wherein the second lock assembly includes a storage medium configured to store a blockchain application and the distributed blockchain, and the blockchain application is configured to utilize the distributed blockchain to effect operation of the second lock assembly.

3. A system comprising:

at least one processor;

at least one storage medium;

a blockchain application stored in the at least one storage medium and executed by the at least one processor;

a data file stored in the at least one storage medium and applied by the blockchain application, the data file including a plurality of linked blocks each including a respective transaction data of a plurality of transaction data, wherein each one of the plurality of transaction data includes a respective event and a time stamp;

a blockchain application stored in the at least one storage medium, executed by the at least one processor, and configured to output an authorization based on a current grant event of a transaction data of the plurality of transaction data;

a lock assembly; and

a digital key adapted to operate the lock assembly, wherein at least one of the lock assembly and the digital key is configured to receive the authorization in order for the digital key to operate the lock assembly.

4. The system set forth in claim 3, further comprising:

a server including a processor of the at least one processor and a storage medium of the at least one storage medium, wherein the block chain application is stored in the storage medium and executed by the processor.

5. The system set forth in claim 4, wherein the server is remote from the lock assembly.

6. The system set forth in claim 5, wherein the lock assembly includes a processor of the at least one processor and is configured to send a transaction data signal indicative of an event and to the processor of the server toward growth of the plurality of the plurality of linked blocks.

7. The system set forth in claim 3, wherein the digital key is a key application loaded into a smart phone.

8. The system set forth in claim 6, wherein the digital key is a key application loaded into a smart phone, and the smart phone is configured to wirelessly send an access command to the lock assembly.

9. The system set forth in claim 3, wherein the plurality of transaction data includes a grant transaction data including a grant event, a key address, a lock address, and a time stamp.

10. The system set forth in claim 3, wherein the plurality of transaction data includes an unlock transaction data including an unlock event, a key address, a lock address, and a time stamp.

11. The system set forth in claim 9, wherein the plurality of transaction data includes an unlock transaction data including an unlock event, a key address, a lock address, and a time stamp.

12. The system set forth in claim 3, wherein the plurality of transaction data includes a lock transaction data including a lock even, a lock address, and a time stamp.

13. The system set forth in claim 11, wherein the plurality of transaction data includes a lock transaction data including a lock even, a lock address, and a time stamp.

14. The system set forth in claim 3, wherein the plurality of transaction data includes an access deny transaction data including an access deny event, a key address, a lock address, and a time stamp.

15. A method of operating a lock system comprising:

applying a digital key to a lock assembly to effect an unlock event;

sending an authorization request communication by the lock assembly to a control arrangement;

applying a blockchain application by the control arrangement to verify the authorization request;

sending an access verification to the lock assembly;

unlocking the lock assembly;

sending an unlock event signal to the blockchain application, wherein the unlock event signal includes an unlock event, a lock assembly address, and a key address;

creating unlock transaction data indicative of the unlock event signal by the blockchain application; and

configuring the unlock transaction data as a block of a plurality of linked blocks and applying a time stamp by the blockchain application.

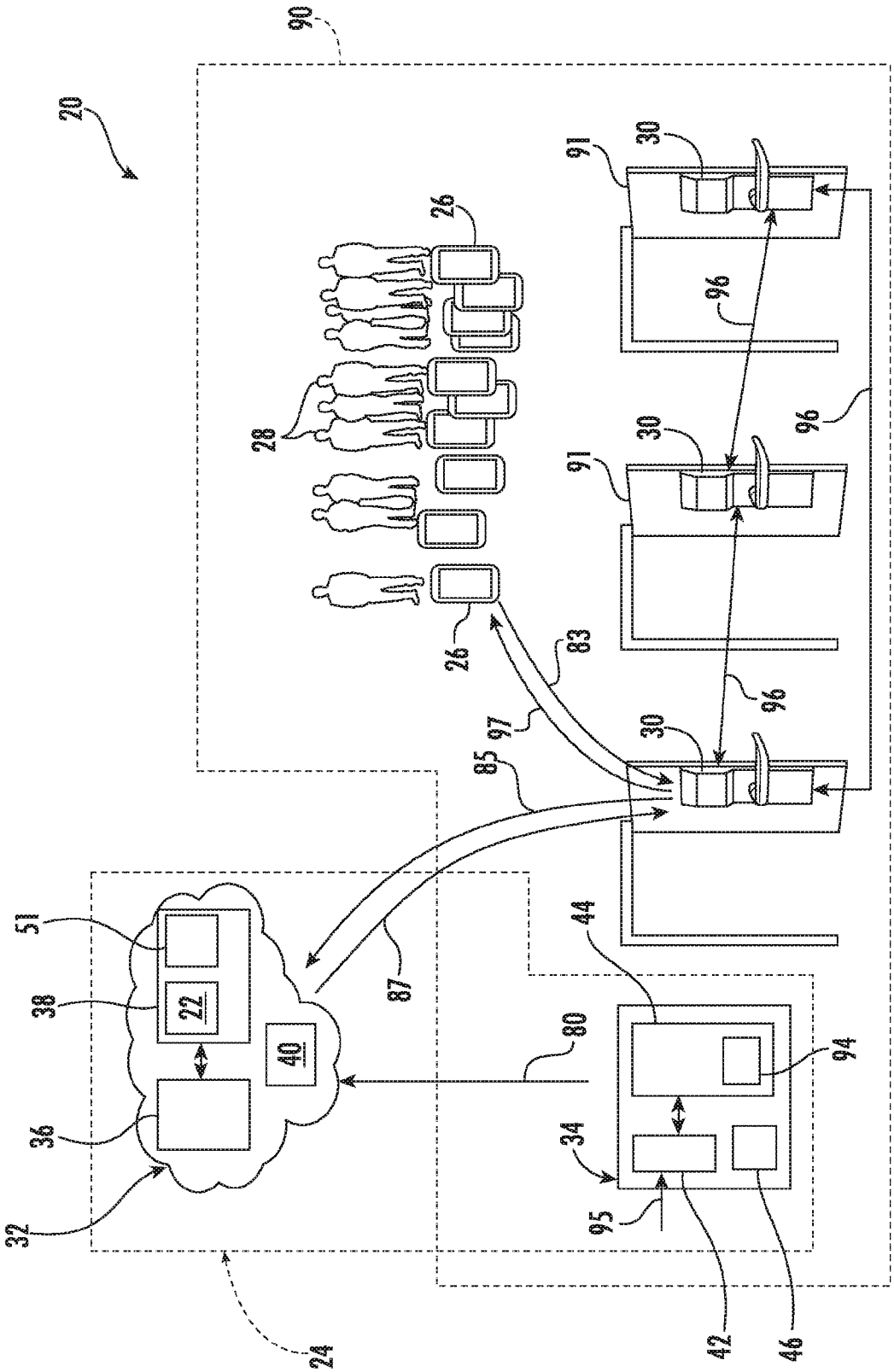
90
20
91
30
96
26
28
83
97
85
87
51
38
22
40
36
32
24
44
80
94
34
95
42
46

FIG. 1

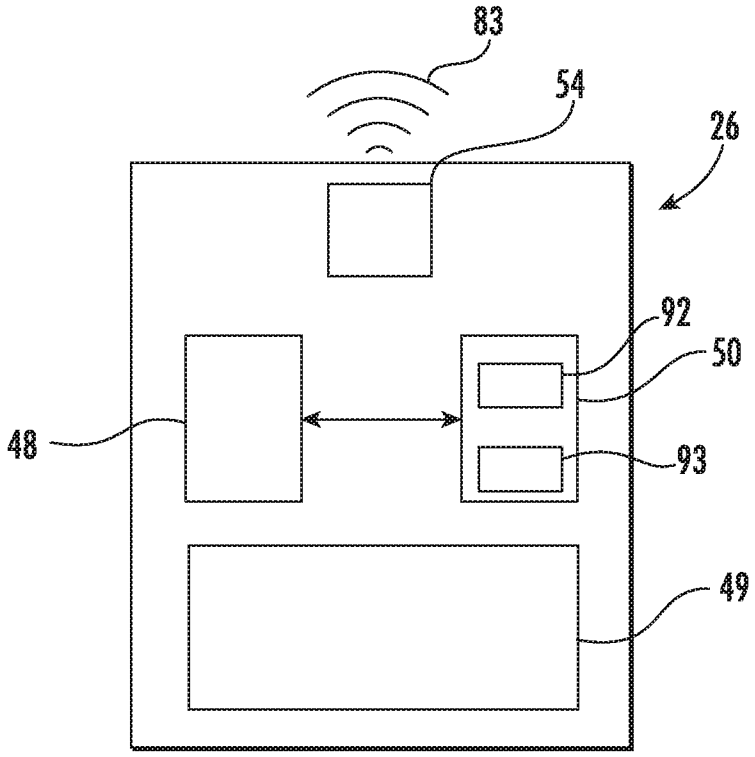

FIG. 2

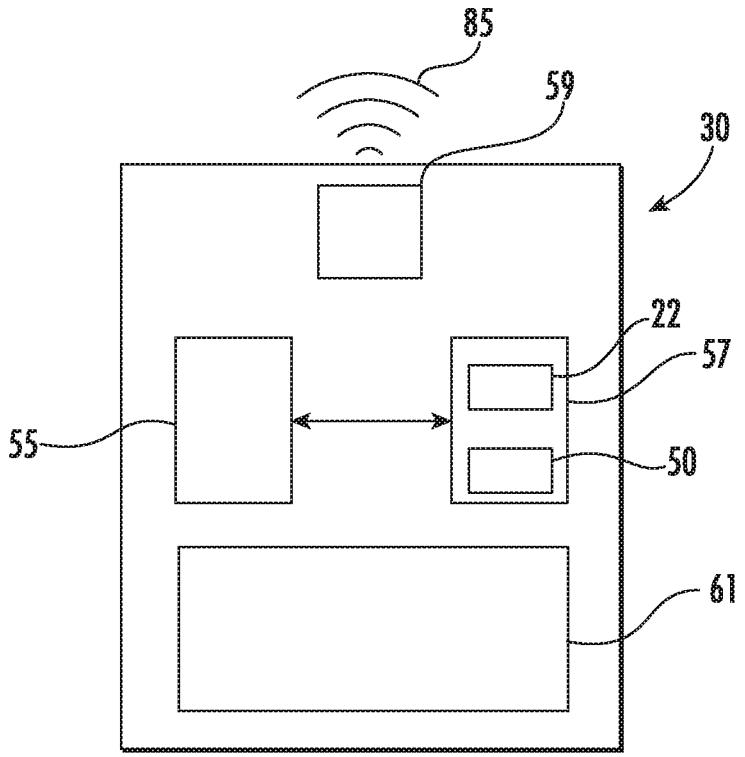

FIG. 3

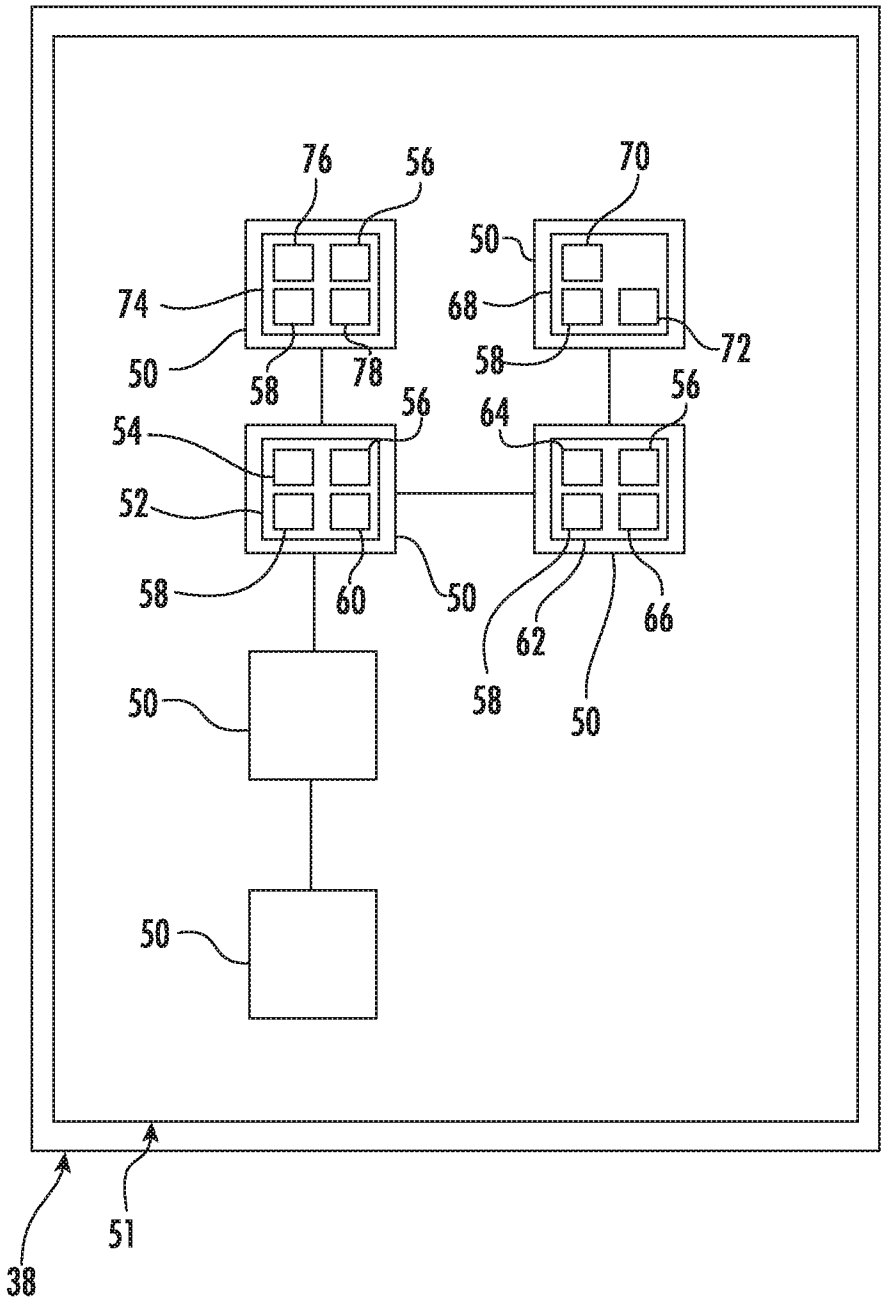
76
56
70
50
74
68
72
58
50
58
78
58
56
64
56
54
52
58
60
50
62
66
58
50
50
50
51
38

FIG. 4

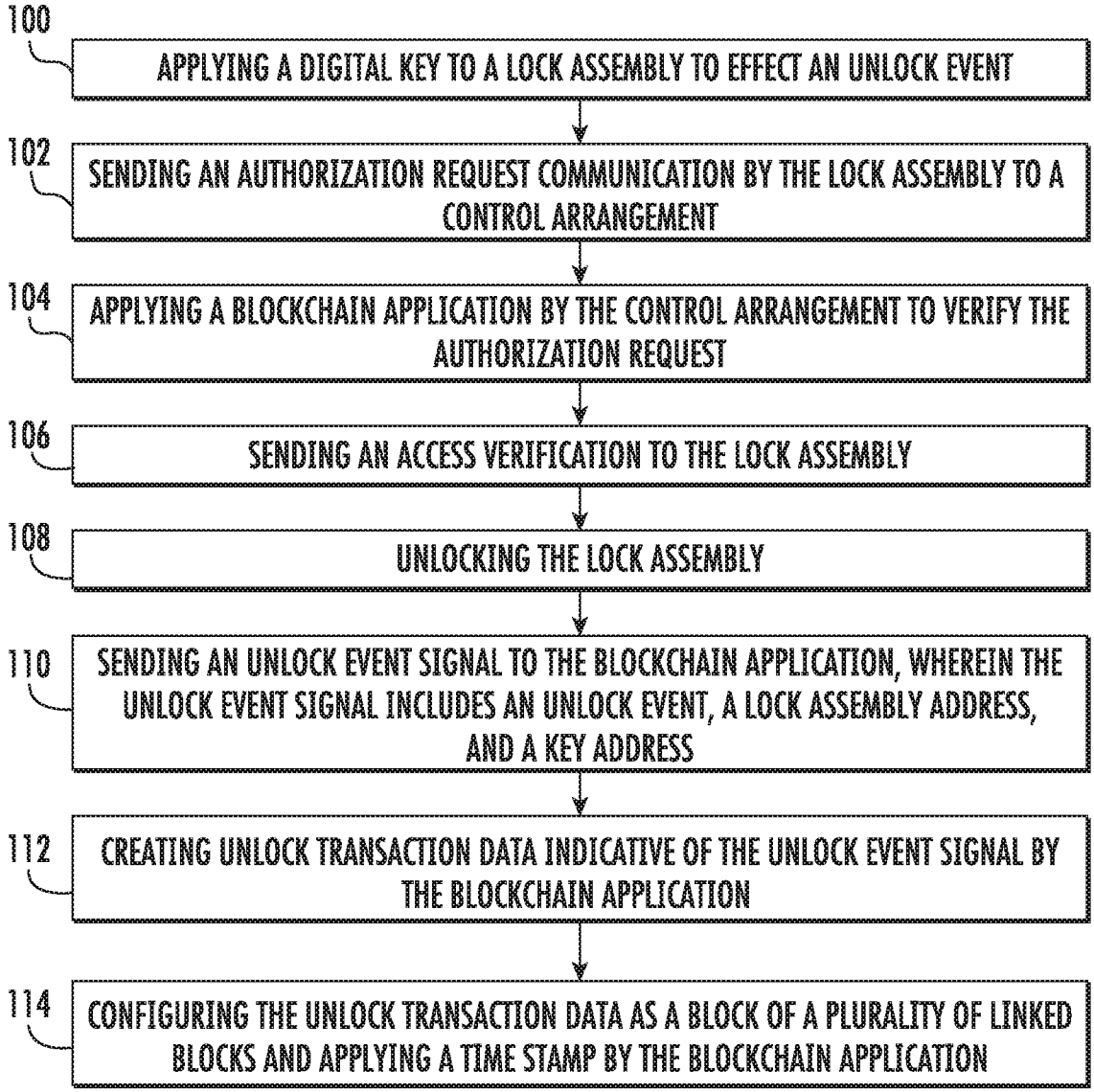
100
APPLYING A DIGITAL KEY TO A LOCK ASSEMBLY TO EFFECT AN UNLOCK EVENT
102
SENDING AN AUTHORIZATION REQUEST COMMUNICATION BY THE LOCK ASSEMBLY TO A CONTROL ARRANGEMENT
104
APPLYING A BLOCKCHAIN APPLICATION BY THE CONTROL ARRANGEMENT TO VERIFY THE AUTHORIZATION REQUEST
106
SENDING AN ACCESS VERIFICATION TO THE LOCK ASSEMBLY
108
UNLOCKING THE LOCK ASSEMBLY
110
SENDING AN UNLOCK EVENT SIGNAL TO THE BLOCKCHAIN APPLICATION, WHEREIN THE UNLOCK EVENT SIGNAL INCLUDES AN UNLOCK EVENT, A LOCK ASSEMBLY ADDRESS, AND A KEY ADDRESS
112
CREATING UNLOCK TRANSACTION DATA INDICATIVE OF THE UNLOCK EVENT SIGNAL BY THE BLOCKCHAIN APPLICATION
114
CONFIGURING THE UNLOCK TRANSACTION DATA AS A BLOCK OF A PLURALITY OF LINKED BLOCKS AND APPLYING A TIME STAMP BY THE BLOCKCHAIN APPLICATION

FIG. 5

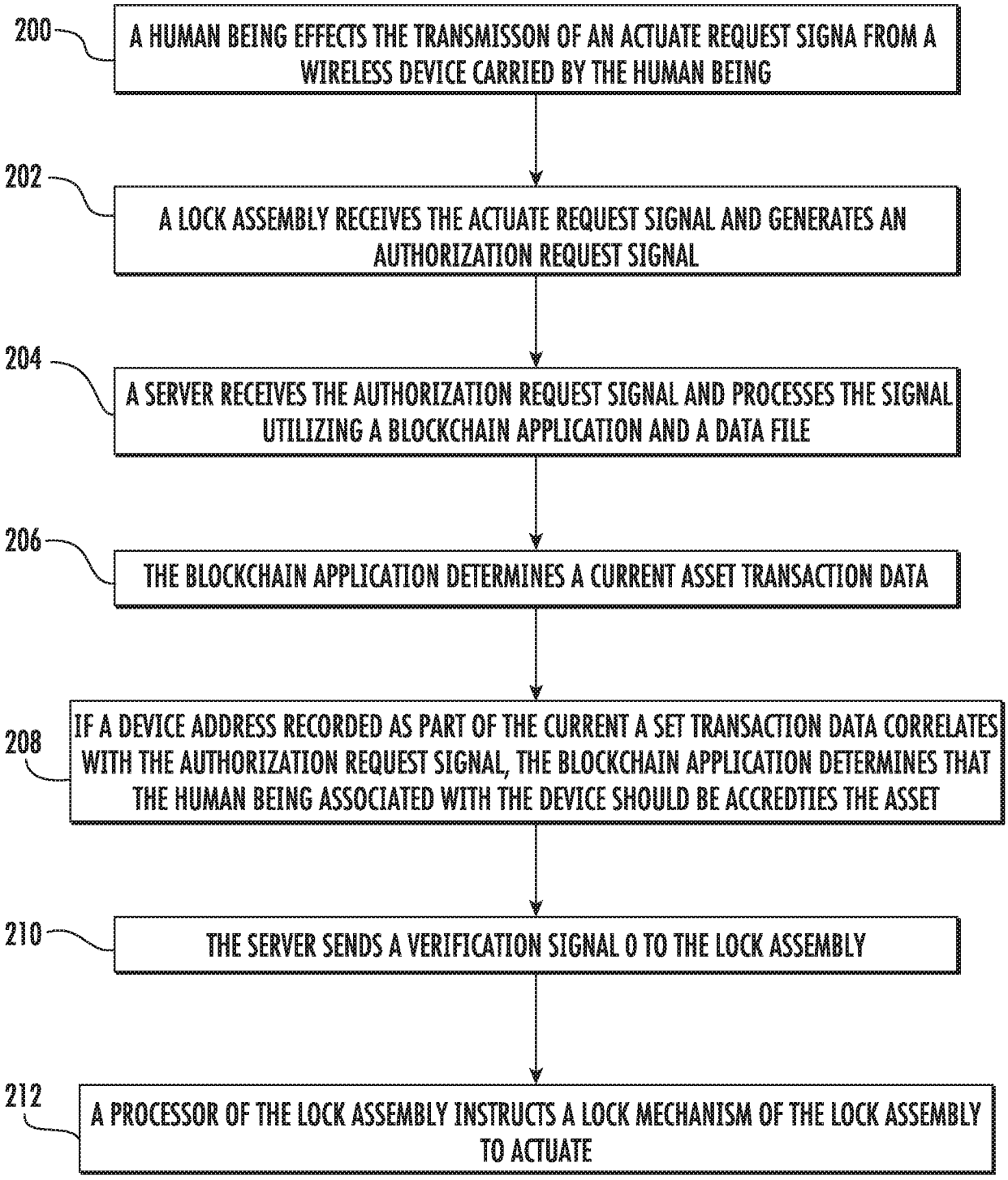
200
A HUMAN BEING EFFECTS THE TRANSMISSON OF AN ACTUATE REQUEST SIGNA FROM A WIRELESS DEVICE CARRIED BY THE HUMAN BEING
202
A LOCK ASSEMBLY RECEIVES THE ACTUATE REQUEST SIGNAL AND GENERATES AN AUTHORIZATION REQUEST SIGNAL
204
A SERVER RECEIVES THE AUTHORIZATION REQUEST SIGNAL AND PROCESSES THE SIGNAL UTILIZING A BLOCKCHAIN APPLICATION AND A DATA FILE
206
THE BLOCKCHAIN APPLICATION DETERMINES A CURRENT ASSET TRANSACTION DATA
208
IF A DEVICE ADDRESS RECORDED AS PART OF THE CURRENT A SET TRANSACTION DATA CORRELATES WITH THE AUTHORIZATION REQUEST SIGNAL, THE BLOCKCHAIN APPLICATION DETERMINES THAT THE HUMAN BEING ASSOCIATED WITH THE DEVICE SHOULD BE ACCREDTIES THE ASSET
210
THE SERVER SENDS A VERIFICATION SIGNAL 0 TO THE LOCK ASSEMBLY
212
A PROCESSOR OF THE LOCK ASSEMBLY INSTRUCTS A LOCK MECHANISM OF THE LOCK ASSEMBLY TO ACTUATE

FIG. 6

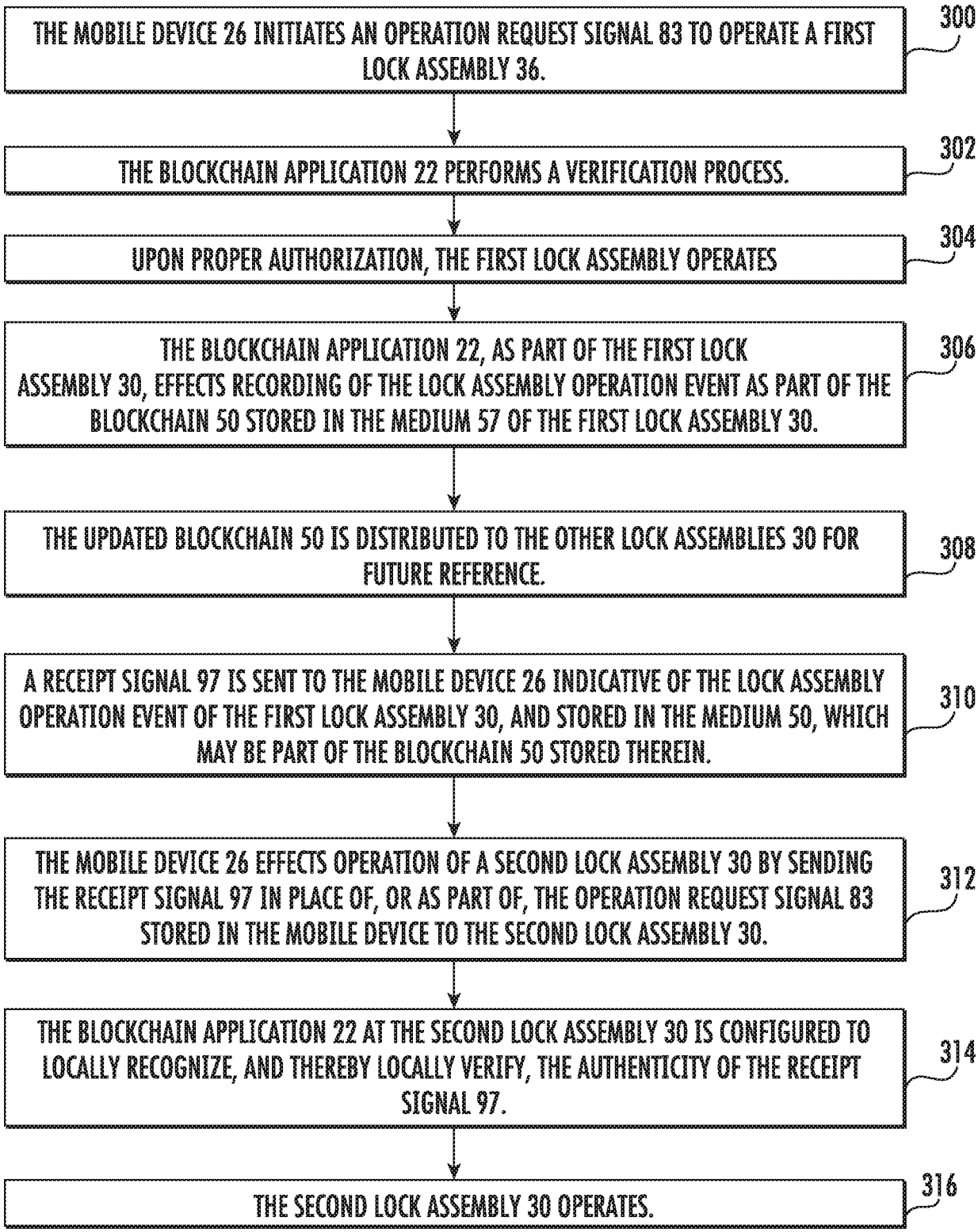
THE MOBILE DEVICE 26 INITIATES AN OPERATION REQUEST SIGNAL 83 TO OPERATE A FIRST LOCK ASSEMBLY 36.
300
THE BLOCKCHAIN APPLICATION 22 PERFORMS A VERIFICATION PROCESS.
302
UPON PROPER AUTHORIZATION, THE FIRST LOCK ASSEMBLY OPERATES
304
THE BLOCKCHAIN APPLICATION 22, AS PART OF THE FIRST LOCK ASSEMBLY 30, EFFECTS RECORDING OF THE LOCK ASSEMBLY OPERATION EVENT AS PART OF THE BLOCKCHAIN 50 STORED IN THE MEDIUM 57 OF THE FIRST LOCK ASSEMBLY 30.
306
THE UPDATED BLOCKCHAIN 50 IS DISTRIBUTED TO THE OTHER LOCK ASSEMBLIES 30 FOR FUTURE REFERENCE.
308
A RECEIPT SIGNAL 97 IS SENT TO THE MOBILE DEVICE 26 INDICATIVE OF THE LOCK ASSEMBLY OPERATION EVENT OF THE FIRST LOCK ASSEMBLY 30, AND STORED IN THE MEDIUM 50, WHICH MAY BE PART OF THE BLOCKCHAIN 50 STORED THEREIN.
310
THE MOBILE DEVICE 26 EFFECTS OPERATION OF A SECOND LOCK ASSEMBLY 30 BY SENDING THE RECEIPT SIGNAL 97 IN PLACE OF, OR AS PART OF, THE OPERATION REQUEST SIGNAL 83 STORED IN THE MOBILE DEVICE TO THE SECOND LOCK ASSEMBLY 30.
312
THE BLOCKCHAIN APPLICATION 22 AT THE SECOND LOCK ASSEMBLY 30 IS CONFIGURED TO LOCALLY RECOGNIZE, AND THEREBY LOCALLY VERIFY, THE AUTHENTICITY OF THE RECEIPT SIGNAL 97.
314
THE SECOND LOCK ASSEMBLY 30 OPERATES.
316

FIG. 7

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2019/064729

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/35 G07C9/00
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)
H04L G06F G07C

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 2018/191714 A1 (JENTZSCH CHRISTOPH [DE] ET AL) 5 July 2018 (2018-07-05) paragraph [0018] - paragraph [0029]; figures 1a,3 paragraph [0049] - paragraph [0053]	1-15
A	MEHRDAD SALIMITARI ET AL: "An Overview of Blockchain and Consensus Protocols for IoT Networks", ARXIV.ORG, CORNELL UNIVERSITY LIBRARY, 201 OLIN LIBRARY CORNELL UNIVERSITY ITHACA, NY 14853, 15 September 2018 (2018-09-15), XP080917565, the whole document	1-15

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
6 March 2020	16/03/2020

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	Mäenpää, Jari

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2019/064729

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2018191714 A1	05-07-2018	CN 110800004 A	14-02-2020
		EP 3563325 A1	06-11-2019
		KR 20190119581 A	22-10-2019
		US 2018191714 A1	05-07-2018
		WO 2018126059 A1	05-07-2018