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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 February 2020 (13.02.2020)

WIPO | PCT

(10) International Publication Number
WO 2020/032937 A1

(51) International Patent Classification:
*G06F 21/62* (2013.01) *G06F 17/30* (2006.01)
*H04L 9/32* (2006.01) *H04L 29/06* (2006.01)

(21) International Application Number:
PCT/US2018/045682

(22) International Filing Date:
07 August 2018 (07.08.2018)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **CISCO TECHNOLOGY, INC.** [US/US]; 170 West Tasman Drive, San Jose, California 95134 (US).

(72) Inventors: **ROBERTS, Christopher Shaun**; 19542 Juniper Breeze Lane, Spring, Texas 77379 (US). **KUNJAN, Solomon Ayyankulankara**; 15 Pilgrim Drive, Unit B, Westford, Massachusetts 01886 (US). **NATARAJAN, Muhilan**; 1306 Monahans Dr., Allen, Texas 75013 (US). **O'BRIEN, Michael P.**; 563 Laurel Cherry Ln., Venice, Florida 34293 (US).

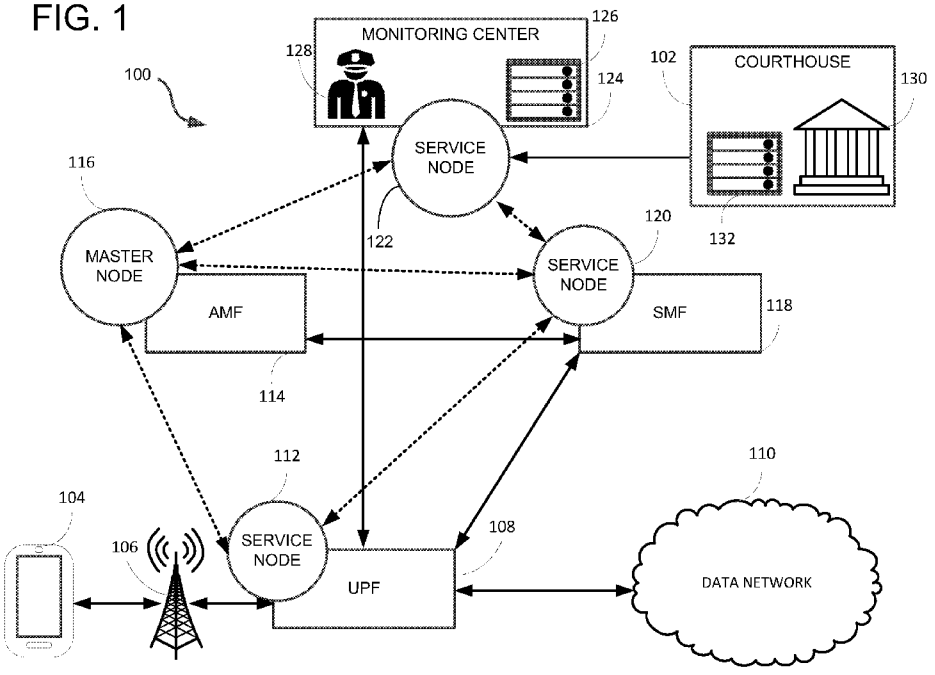
(74) Agent: **MCKNIGHT, Brian**; Polsinelli PC, Three Embarcadero Center, Suite 2400, San Francisco, California 95111 (US).

(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,

(54) Title: SYSTEM AND METHOD FOR ACCESSING A DATA REPOSITORY

FIG. 1




(57) Abstract: Access to a data repository can be managed by an administration service linked to a blockchain network including at least one service node and a master node. The service node receives from an authorizing device a root block having a digital authorization for access data in the data repository. The master node transmits a consensus protocol to the service node. When an accessing device requests access to the data of the data repository, the service node verifies an access right of the accessing device according to the consensus protocol. A record of access to the data repository by the accessing device is generated and includes a reference to the root block. The record is then stored.

WO 2020/032937 A1

*[Continued on next page]*

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).

**Declarations under Rule 4.17:**

— *of inventorship (Rule 4.17(iv))*

**Published:**

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

# SYSTEM AND METHOD FOR ACCESSING A DATA REPOSITORY

## TECHNICAL FIELD

**[0001]** The present technology pertains to accessing data repositories; and more specifically to a system using a distributed database for verifying access to data repositories by law enforcement agencies.

## BACKGROUND

**[0002]** As mobile networking advances, user plane control continues to move closer to radio towers and the like (e.g., NodeB, etc.), and further away from centrally located data centers and the like. The increasingly distributed nature of mobile networking can make validation and tracking an onerous and tedious task. Distributed network architectures also create potentially greater security risks. For example, call data access requests and interceptions must be validated at various points within a network and, furthermore, those network points may vary between requests and such. Where validation and granting of access requests is accomplished via manual inspection, it can take considerable time to interact with the various points within the network and recordation of the requests and granted access may be inconsistent or even nonexistent. As a result, managing authorized or lawful access to data sources over mobile networks can be challenging. Furthermore, it may be difficult to achieve a comprehensive record of which authorities or agencies have accessed, or attempted to access, a data repository.

## BRIEF DESCRIPTION OF THE DRAWINGS

**[0003]** In order to describe the manner in which the above-recited and other advantages and features of the disclosure can be obtained, a more particular description of the principles briefly described above will be rendered by reference to specific embodiments thereof which are illustrated in the appended drawings. Understanding that these drawings depict only exemplary embodiments of the disclosure and are not therefore to be considered to be limiting of its scope, the principles herein are described and explained with additional specificity and detail through the use of the accompanying drawings in which:

**[0004]** FIG. 1 illustrates an example network environment, according various embodiments of the subject technology;

**[0005]** FIG. 2 illustrates an example network environment, according to various embodiments of the subject technology;

**[0006]** FIG. 3 depicts an example method, according to various embodiments of the subject technology;

**[0007]** FIG. 4 depicts an example blockchain network, according to various embodiments of the subject technology;

**[0008]** FIG. 5 illustrates an example computing device, according to various embodiments of the subject technology; and

**[0009]** FIG. 6 illustrates an example computing device, according to various embodiments of the subject technology.

## DESCRIPTION OF EXAMPLE EMBODIMENTS

**[0010]** Various embodiments of the disclosure are discussed in detail below. While specific implementations are discussed, it should be understood that this is done for illustration purposes only. A person skilled in the relevant art will recognize that other components and configurations may be used without parting from the spirit and scope of the disclosure. Thus, the following description and drawings are illustrative and are not to be construed as limiting. Numerous specific details are described to provide a thorough understanding of the disclosure. However, in certain instances, well-known or conventional details are not described in order to avoid obscuring the description. References to one or an embodiment in the present disclosure can be references to the same embodiment or any embodiment; and, such references mean at least one of the embodiments.

**[0011]** Reference to "one embodiment" or "an embodiment" means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of the disclosure. The appearances of the phrase "in one embodiment" in various places in the specification are not necessarily all referring to the same embodiment, nor are separate or alternative embodiments mutually exclusive of other embodiments. Moreover, various features are described which may be exhibited by some embodiments and not by others.

**[0012]** The terms used in this specification generally have their ordinary meanings in the art, within the context of the disclosure, and in the specific context where each term is used.

Alternative language and synonyms may be used for any one or more of the terms discussed herein, and no special significance should be placed upon whether or not a term is elaborated or discussed herein. In some cases, synonyms for certain terms are provided. A recital of one or more synonyms does not exclude the use of other synonyms. The use of examples anywhere in this specification including examples of any terms discussed herein is illustrative only, and is not intended to further limit the scope and meaning of the disclosure or of any example term. Likewise, the disclosure is not limited to various embodiments given in this specification.

**[0013]** Without intent to limit the scope of the disclosure, examples of instruments, apparatus, methods and their related results according to the embodiments of the present disclosure are given below. Note that titles or subtitles may be used in the examples for convenience of a reader, which in no way should limit the scope of the disclosure. Unless otherwise defined, technical and scientific terms used herein have the meaning as commonly understood by one of ordinary skill in the art to which this disclosure pertains. In the case of conflict, the present document, including definitions will control.

**[0014]** Additional features and advantages of the disclosure will be set forth in the description which follows, and in part will be obvious from the description, or can be learned by practice of the herein disclosed principles. The features and advantages of the disclosure can be realized and obtained by means of the instruments and combinations particularly pointed out in the appended claims. These and other features of the disclosure will become more fully apparent from the following description and appended claims, or can be learned by the practice of the principles set forth herein.

## OVERVIEW

**[0015]** A blockchain can be used to securely access and manage access to data sources in a scalable manner. The data sources can be repositories, logs, data streams, and the like and the blockchain, and an associated blockchain network, may authorize, validate, and record access requests, both successful and unsuccessful, to each respective data source.

**[0016]** Furthermore, in some embodiments, lawful authorization for accessing data can be maintained via the blockchain network. For example, a judge can authorize various law enforcement agencies to access call data (e.g., wiretap and the like) of a suspect. The judicial authorization may be used as a root block for a blockchain for tracking all access to the call

data of the suspect under the judicial authorization. In some examples, the root block can include various parameters such as authorized agencies, authorized individuals, a time window for the authorization, and other content. Each access to the call data can be maintained as an entry on the blockchain and so may be reviewed at a later date with a decreased likelihood that the records have been altered due to the cryptographically interlinked nature of records on a blockchain.

**[0017]** In one embodiment, an administration service may manage access to a data repository or source. One or more blockchain service nodes can be part of a blockchain network and linked to the administration service for validating and storing copies of digital authorizations for law enforcement agencies (LEAs). Each digital authorization may be stored in a root block of a blockchain and the root block can be generated by a device controlled by a judge and able to provide a cryptographic key associated with the judge as well as an identification of the data repository or source and access parameters also within the root block.

**[0018]** In one embodiment, a master node can be a part of the blockchain network in order to define consensus requirements across the network for access to the data repository by a law enforcement agency and the like via an access device. The access device, controllable by the law enforcement agency, may transmit access requests with regards to the data repository to a blockchain service node which may verify, according to the consensus requirements defined by the master node, that the law enforcement agency is authorized to access the data repository. Furthermore, the blockchain service node may generate a data access record related to the access request and link the record to the root block via, for example, the blockchain (e.g., by appending the record as a block and the like).

## EXAMPLE EMBODIMENTS

**[0019]** Authorized access to data repositories, such as, for example and without imputing limitation, in the case of law enforcement retrieving call data for a cellphone belonging to a suspect, can be automated across mobile network environments, such as 5G mobile core and the like. In some embodiments, a blockchain can be used to secure and create an audit trail of government agencies and the like accessing call data associated with suspect cellphones.

**[0020]** Abuse of power in government agencies or service providers may be controlled and monitored through tracking and recording of data access over the blockchain. Recorded data

access can be entered onto the blockchain and audited at a later time. Furthermore, the blockchain may provide an increased certainty that the record has not been tampered with.

**[0021]** The blockchain may include a root block having an official authorization and, in some embodiments, other parameters such as, for example and without imputing limitation, specific agency authorization, specific investigator authorization, duration, content, and the like. Accordingly, a law enforcement agency and the like seeking access to call data may have their respective authorization for access checked against the root block of the blockchain.

**[0022]** In order to generate the root block, a specialized software application may be executed by a device under control of a court system. For example, a judge may provide to the specialized software application a digital court order which may be authenticated based on a cryptographic signature such as a "pretty good privacy" (PGP) public key and private key pairing and the like. The root block can then be transmitted to a blockchain network made up of various service nodes controlled by law enforcement agencies, service providers, and the like. In some embodiments, the digital court order may be verified authenticated via two-factor authentication (2FA) and the like.

**[0023]** Furthermore, a variable consensus protocol can be enforced by a master node on the blockchain network. In other words, different blockchains, and thus different authorizations, can be validated according to different consensus protocols as defined by the master node. In one example, a warrant under the Foreign Intelligence Surveillance Act (or a "FISA warrant") may be validated only by certain service nodes within the blockchain network, whereas a standard warrant issued by a district court in a state jurisdiction may be validated by the network at large or by service nodes within the same geographical jurisdiction and the like.

**[0024]** FIG. 1 depicts a network environment 100 over which a blockchain can provide recorded and authorized access to data sources such as call data. The call data may originate from a cellphone 104 in communication with a data network 110 over a radio network and the like provided by a cell tower 106. Data transmissions to and from cellphone 104 may be managed by a user plane function (UPF) 108.

**[0025]** In one embodiment, user plane function (UPF) 108 provides packet routing, network interconnection (e.g., such as to data network 110), policy enforcement such as Quality of

Service (QoS) and the like, and other functions for managing user access and data across a network. User plane function (UPF) 108 may include various subsystems, applications, and subnetworks as will be apparent to a person having ordinary skill in the art.

**[0026]** A session management function (SMF) 118 may communicate with user plane function (UPF) 108 in order to manage communication sessions involving in cellphone 104. For example, a phone call, over voice over internet protocol (VOIP) or telephone network, may be managed by session management function (SMF) 118. In other examples, application-specific data streams, such as streaming video and the like, may be manage by session management function (SMF) 118. Nevertheless, session management function (SMF) 118 may also be in communication with an access and mobility management function (AMF) 114 in order to maintain sessions across locations or network portions. Access and mobility management function (AMF) 114 may manage, for example, maintaining a VOIP session for cellphone 104 as it travels between network coverage areas such as for a commuter participating in a phone call while on a moving train and the like.

**[0027]** In one embodiment, user plane function (UPF) 108 may also be in communication with a monitoring center 124. Monitoring center 124 may be a law enforcement agency installation and the like and can include a server 124 for monitoring phone calls of suspects and the like. An investigating officer 128 may use the server 124 in order to intercept data transmissions from cellphone 104. In one embodiment, monitoring center 124 may receive a copy of call data transmitted by cellphone 104 via user plane function (UPF) 108 via routing of copied data, log information, *post hoc* records, and the like as will be apparent to a person having ordinary skill in the art.

**[0028]** An authority, such as a courthouse 102, may provide permission and/or grant authority to monitoring center 126 or investigating officer 128 to intercept calls from cellphone 104. In some embodiments, courthouse 102 includes a court 130 and associated authorizing device 132. Authorizing device can be a computer terminal, server, executable application, and the like as will be apparent to a person having ordinary skill in the art.

**[0029]** Authorizing device 132 may transmit to a blockchain network a root block containing authorization, such as a cryptographic signature and the like, from a judge as well as warrant parameters for permitting law enforcement agencies to intercept data from cellphone 104. The blockchain network may include a number of nodes overlaid onto, for example, user plane function (UPF) 108, access and mobility management function (AMF) 114, session

management function (SMF) 118, and monitoring center 124. While four nodes are depicted in FIG. 1, it will be understood by a person having ordinary skill in the art that any number of nodes may be included in the blockchain network. Further, in some examples, network functions or endpoints may include multiple nodes. For example, session management function (SMF) 118 may include service node 120 as well as, in some examples, multiple other service nodes.

**[0030]** Here, for explanatory purposes only, each network function and endpoint houses only a single node. Monitoring center 124 houses service node 122, session management function (SMF) 118 houses service node 120, user plane function (UPF) 108 houses service node 112, and access and mobility management function (AMF) 114 houses master node 116. In one example, the blockchain network is fully interconnected. That is to say, each node 112, 116, 120, 122 may communicate with each and every other node. In some other examples, nodes may communicate with a portion of other nodes in the blockchain network and through, for example, overlapping portions, all nodes in the blockchain network may indirectly intercommunicate.

**[0031]** In one embodiment, authorizing device 132 transmits the root block to service node 122 (housed by monitoring center 126). In some examples, the root block may be transmitted to service node 122 via an encrypted tunnel such as through Secure Shell (SSH) protocol and such. Service node 122 then transmits to master node 116 the received root block for dissemination to service nodes 112, 120, 122 of the blockchain network. In one embodiment, master node 116 transmits the root block to each service node 112, 120, 122 via respective encrypted tunnels. For example, service nodes 112, 120, and 122 may each maintain a cache of all root blocks received from master node 116 through an encrypted tunnel.

**[0032]** When investigating officer 128 attempts to intercept call data from cellphone 104, a root block associated with cellphone 104 may be checked at service node 122. Before user plane function (UPF) 108 provides access to investigating officer 128, service node 122 or 112 may validate the veracity and/or accuracy of the root block against copies stored in other nodes according to a consensus protocol stored by master node 116. Master node 116 may store multiple consensus protocols which may be utilized based on, for example, data stored a particular root block. In one embodiment, service nodes 122 or 112 may query master node 116 for an appropriate consensus protocol and then execute validation based on that. One such consensus protocol, provided for explanatory purposes and in no way limiting, may be

to check a hash value for copies of the respective root block at each other node across the blockchain network. If all hashes are identical, service node 122 or 112 may regard the root block as valid and thus investigating office 128, if authorized by the contents of the root block, to be permitted to access call data from cellphone 104.

**[0033]** Furthermore, in one embodiment, a record of investigating officer 128 can be generated by service node 122 and then linked to the root block in order to generate or grow a blockchain providing a ledger of accesses and/or access attempts by investigating officer 128 and other law enforcement agencies. Further, the updated blockchain may be disseminated across the blockchain network in order to maintain consistency between nodes.

**[0034]** Nodes 112, 116, 120, and 122 may be located in different jurisdictions and thus the blockchain network may be international in nature. Likewise, courthouse 102 and/or monitoring center 124 may be in a different jurisdiction than each other and/or cellphone 104. FIG. 2 depicts one such embodiment of a multi-jurisdiction blockchain network 200 spanning the United States and Canada.

**[0035]** Each service provider 202, 206, and 210 may include a portion of network environment 100. For example, each service provider 202, 206, and 210 may include a respective user plane function (UPF) 108, session management function (SMF) 118, and/or access and mobility management function (AMF) 114, each with respective service nodes 112, 120, and/or master node 116. Further, law enforcement agencies 204, 208, and 212 may each be in jurisdictions of varying differences. For example, law enforcement agency 204 and law enforcement agency 208 may each be in different states within the United States and thus investigations across state borders may require varying types of authorization to retrieve call data through different parts of respective networks controlled by service providers 202 and 206.

**[0036]** Similarly, service provider 210 may be in an altogether different national jurisdiction from service providers 202 and 206 or law enforcement agencies 204 and 208. However, a user plane function (UPF) 108 of service provider 210 may use include a respective service node 112 and thus may automatically validate and verify, for example, a warrant complying with an international standard or jurisdiction in order to access call data of cellphone 104 while located in, for example, Canada.

**[0037]** FIG. 3 depicts a method 300 by which, for example and without imputing limitation, an investigating agent 128 can gain authorized and documented access to a repository of data, such as call data for cellphone 104.

**[0038]** In one embodiment, an authorization for accessing a data repository may first be received by, for example, authorizing device 132 (operation 302). In some embodiments, the authorization includes a digital key provided by a judge controlling authorizing device 132. Furthermore, in various examples and embodiments, other access parameters such as time-frames, identification of particular law enforcement agencies, and the like may be included along with an identification of the data repository. The identification of the data repository can be a device identifier, phone number identifier, or other identifier as will be apparent to a person having ordinary skill in the art.

**[0039]** In some embodiments, authorizing device 132 and the like may construct a root block consisting of the received information such as, for example, the authorization (operation 304). The root block may be in various forms suitable for transmission and processing such as, for example and without imputing limitation, a JavaScript Object Notation (JSON) object, serialized data object structure, a tuple, a dict or other key-value structure, or various other data structures as will be apparent to a person having ordinary skill in the art.

**[0040]** The root block may then be distributed to nodes on a blockchain network (operation 306). In some embodiments, one service node (e.g., service node 122) may receive the root block from authorizing device 132. The service node (e.g., service node 122) can then redistribute the received root block to a master node (e.g., master node 116), which then disseminates the root block to each service node in the blockchain network through, for example and without imputing limitation, encrypted tunnels. In some embodiments, each or multiple service nodes may receive the root block directly from authorizing device 132. Nevertheless, each node in the blockchain network may eventually store a copy of the root block (and associated blockchain, as discussed below).

**[0041]** A service node (e.g., service node 122) may receive a request, from an accessing device such as server 124 and the like, to access the data repository (operation 308). In some embodiments, the accessing device may be associated with a service node on the blockchain network. In some embodiments, the service node receiving the request may be associated with a routing and flow control portion of a service provider network (e.g., user plane

function (UPF) 108) and so can receive the request via a user plane function (UPF) and the like rather than directly from the accessing device.

**[0042]** In any case, the service node may verify that the accessing device has access rights, or authorization, to the data repository by examining the earlier received root block and applying a consensus protocol (operation 310). The consensus protocol may be determined by a master node within the blockchain network and can define a network consensus requirement for accessing the data repository associated with the root block. For example, the master node may select, based on preconfigured rules or according to a determination based on processing the root block and/or network, a subset of service nodes within the blockchain network to validate the root block and/or blockchain of the root block. The master node can send a command to validate, via encrypted tunnel, to each service node of the selected subset of service nodes. In one embodiment, the command may contain identification of other service nodes for validation (e.g., a list of service node IP addresses) and each service node of the subset of service nodes may communicate with each other service node of the subset of service nodes through an encrypted IP tunnel and the like.

**[0043]** In further response to the master node command, the service nodes may transmit back whether the validation was successful. Depending on the consensus protocol, the master node may verify the access right or not. For example, the master node may verify the access right only if all selected service nodes respond with a successful validation. In another example, a consensus protocol for a particular root block may include a 75% consensus requirement for validating access rights. That is to say, 75% or more of other verifying nodes each have identical copies of the root block in order to successfully verify access requests routed through it. In some embodiments, consensus protocols may vary based on characteristics of the root block and/or an associated blockchain.

**[0044]** In some embodiments, if an access right cannot be verified (e.g., due to being unable to validate a respective blockchain, etc.), then the accessing device may be barred from further access to the network pending investigation and an encrypted alert can be transmitted to the master node. The authorizing device (e.g., an issuing court, etc.), relevant service providers, and accessing device (e.g., law enforcement agency, etc.) may also be alerted. Furthermore, in some embodiments, the service nodes which are unable to verify the access right may be reported through an alert or the like in order to further investigation. In some embodiments, the entire network may shut down to further access requests once a single

failure has been detect or may shut down or otherwise limit requests at some threshold number of failures reported.

**[0045]** In some embodiments, having verified the access right, access to the data repository may be granted to the requesting device and the access can be recorded and linked to the root block as a block in a blockchain depending from the root block (operation 312). Further, in some embodiments, copies of the root block throughout the blockchain network may then be updated to reflect the updated blockchain. In other words, where a root block had, for example, no access requests associated with it before a first access request, it may now be updated across the network by storing in the caches of each service node a new block linked back to the root block (e.g., by including a hash reference and such). Likewise, where there had been a previous access request, a longer blockchain reflecting the new access request may now update be stored in the caches of each service node across the network by storing a new block linked back to a most recent block depending from the root block. In some embodiments, updates to the blockchain may be disseminated by the master node directly to each service node via, for example, respective encrypted IP tunnels. In some embodiments, updates may disseminate across the network via communications between services nodes. In this manner, a growing historical record of accesses under the authorization contained in the original root block may be maintained throughout the network.

**[0046]** While FIG. 4 depicts one specific blockchain network environment 400 of the present disclosure, it is by no means the only blockchain network architecture on which the concepts herein can be implemented. For example, an architecture wherein each access terminal is associated with a network node, etc., can be used. Further, other types of access terminals such as mobile devices, smartphones, and the like could also be used with blockchain network environment 400.

**[0047]** Nodes 404A-C within a blockchain network 402 may intercommunicate and store copies of blockchain and similar data objects in memory. Each node 404A-C can store respective complete copies of each blockchain on the blockchain network 402. Further, while FIG. 4 depicts each node 404A-C as a dedicated server 406A-C, in some examples nodes 404A-C may instead or also be an executable software application on a server and/or personal computer, a virtual machine, and the like.

**[0048]** Terminals 408 and 416 interact with blockchain network 402 via, for example, a secured network (e.g., VPN, etc.). Terminal 408 may update one of the stored blockchains by

transmitting an event transmission, record object, or other signal to node 404C within blockchain network 402. Node 404C may then process the received transmission in order to generate a new block 410 which can be added onto a respective blockchain 412. In some examples, there may be processes for randomizing which node assumes authority to update the blockchain such as, for example, a mining algorithm and the like (e.g., solving an easily verifiable but difficult to solve cryptographic puzzle such as determining appended characters which will cause a hash value to have a particular quality). In other examples, certain or all nodes may be granted authority to update blockchains by the system and any updates produced are taken presumed authentic and authoritative.

**[0049]** Node 404C may transmit an updated blockchain 414 to each other node 404A-B in blockchain network 402. Updated blockchain 414 may include previous blockchain 412 with a new block 410 appended. In this manner, updated blockchain 414 may reflect a sequential expansion of the associated blockchain and may replace previous copies (e.g., copies not including new block 410) stored on the node.

**[0050]** Although the system shown in FIG. 5 is one specific network device of the present disclosure, it is by no means the only network device architecture on which the concepts herein can be implemented. For example, an architecture having a single processor that handles communications as well as routing computations, etc., can be used. Further, other types of interfaces and media could also be used with the network device 500.

**[0051]** Regardless of the network device's configuration, it may employ one or more memories or memory modules (including memory 506) configured to store program instructions for the general-purpose network operations and mechanisms for roaming, route optimization and routing functions described herein. The program instructions may control the operation of an operating system and/or one or more applications, for example. The memory or memories may also be configured to store tables such as mobility binding, registration, and association tables, etc. Memory 506 could also hold various software containers and virtualized execution environments and data.

**[0052]** The network device 500 can also include an application-specific integrated circuit (ASIC), which can be configured to perform routing, switching, and/or other operations. The ASIC can communicate with other components in the network device 500 via the connection 510, to exchange data and signals and coordinate various types of operations by the network device 500, such as routing, switching, and/or data storage operations, for example.

**[0053]** FIG. 6 illustrates a computing system architecture 600 including components in electrical communication with each other using a connection 605, such as a bus. System 600 includes a processing unit (CPU or processor) 610 and a system connection 605 that couples various system components including the system memory 615, such as read only memory (ROM) 620 and random access memory (RAM) 625, to the processor 610. The system 600 can include a cache of high-speed memory connected directly with, in close proximity to, or integrated as part of the processor 610. The system 600 can copy data from the memory 615 and/or the storage device 630 to the cache 612 for quick access by the processor 610. In this way, the cache can provide a performance boost that avoids processor 610 delays while waiting for data. These and other modules can control or be configured to control the processor 610 to perform various actions. Other system memory 615 may be available for use as well. The memory 615 can include multiple different types of memory with different performance characteristics. The processor 610 can include any general purpose processor and a hardware or software service, such as service 1 632, service 2 634, and service 3 636 stored in storage device 630, configured to control the processor 610 as well as a special-purpose processor where software instructions are incorporated into the actual processor design. The processor 610 may be a completely self-contained computing system, containing multiple cores or processors, a bus, memory controller, cache, etc. A multi-core processor may be symmetric or asymmetric.

**[0054]** To enable user interaction with the computing device 600, an input device 645 can represent any number of input mechanisms, such as a microphone for speech, a touch-sensitive screen for gesture or graphical input, keyboard, mouse, motion input, speech and so forth. An output device 635 can also be one or more of a number of output mechanisms known to those of skill in the art. In some instances, multimodal systems can enable a user to provide multiple types of input to communicate with the computing device 600. The communications interface 640 can generally govern and manage the user input and system output. There is no restriction on operating on any particular hardware arrangement and therefore the basic features here may easily be substituted for improved hardware or firmware arrangements as they are developed.

**[0055]** Storage device 630 is a non-volatile memory and can be a hard disk or other types of computer readable media which can store data that are accessible by a computer, such as magnetic cassettes, flash memory cards, solid state memory devices, digital versatile disks,

cartridges, random access memories (RAMs) 625, read only memory (ROM) 620, and hybrids thereof.

**[0056]** The storage device 630 can include services 632, 634, 636 for controlling the processor 610. Other hardware or software modules are contemplated. The storage device 630 can be connected to the system connection 605. In one aspect, a hardware module that performs a particular function can include the software component stored in a computer-readable medium in connection with the necessary hardware components, such as the processor 610, connection 605, output device 635, and so forth, to carry out the function.

**[0057]** For clarity of explanation, in some instances the present technology may be presented as including individual functional blocks including functional blocks comprising devices, device components, steps or routines in a method embodied in software, or combinations of hardware and software.

**[0058]** In some embodiments the computer-readable storage devices, mediums, and memories can include a cable or wireless signal containing a bit stream and the like. However, when mentioned, non-transitory computer-readable storage media expressly exclude media such as energy, carrier signals, electromagnetic waves, and signals per se.

**[0059]** Methods according to the above-described examples can be implemented using computer-executable instructions that are stored or otherwise available from computer readable media. Such instructions can comprise, for example, instructions and data which cause or otherwise configure a general purpose computer, special purpose computer, or special purpose processing device to perform a certain function or group of functions. Portions of computer resources used can be accessible over a network. The computer executable instructions may be, for example, binaries, intermediate format instructions such as assembly language, firmware, or source code. Examples of computer-readable media that may be used to store instructions, information used, and/or information created during methods according to described examples include magnetic or optical disks, flash memory, USB devices provided with non-volatile memory, networked storage devices, and so on.

**[0060]** Devices implementing methods according to these disclosures can comprise hardware, firmware and/or software, and can take any of a variety of form factors. Typical examples of such form factors include laptops, smart phones, small form factor personal computers, personal digital assistants, rackmount devices, standalone devices, and so on.

Functionality described herein also can be embodied in peripherals or add-in cards. Such functionality can also be implemented on a circuit board among different chips or different processes executing in a single device, by way of further example.

**[0061]** The instructions, media for conveying such instructions, computing resources for executing them, and other structures for supporting such computing resources are means for providing the functions described in these disclosures.

**[0062]** Although a variety of examples and other information was used to explain aspects within the scope of the appended claims, no limitation of the claims should be implied based on particular features or arrangements in such examples, as one of ordinary skill would be able to use these examples to derive a wide variety of implementations. Further and although some subject matter may have been described in language specific to examples of structural features and/or method steps, it is to be understood that the subject matter defined in the appended claims is not necessarily limited to these described features or acts. For example, such functionality can be distributed differently or performed in components other than those identified herein. Rather, the described features and steps are disclosed as examples of components of systems and methods within the scope of the appended claims.

Claim language reciting "at least one of" refers to at least one of a set and indicates that one member of the set or multiple members of the set satisfy the claim. For example, claim language reciting “at least one of A and B” means A, B, or A and B.

## CLAIMS

1. A system for managing access to a data repository, the system comprising:

at least one administration service to manage access to a data repository;

at least one blockchain service node configured to validate and store a copy of a digital authorization for accessing data stored in the data repository, the at least one service node linked to the at least one administration service;

an authorizing device configured to transmit a root block to the at least one blockchain service node, the root block comprising the digital authorization for accessing data stored in the data repository and an identification of the data repository;

a master node configured to transmit a consensus protocol to the at least one blockchain service node, the consensus protocol defining a network consensus requirement for access to the data repository pursuant to the digital authorization stored at the at least one blockchain service node; and

an accessing device configured to transmit a request to the at least one service node, the request to access the data repository, and the at least one blockchain service node configured to:

verify, according to the consensus protocol, an access right to the data repository, the access right associated with the accessing device and the digital authorization;

generate a record of access to the data repository by the accessing device, the record of access including a reference to the root block either directly or indirectly through at least one other record including a reference to the root block; and

store the record of access.

2. The system of claim 1, further comprising a plurality of service nodes each configured to validate and store a copy of the digital authorization to access data stored in the data repository, and wherein the consensus protocol includes comparing the respective copies to each other.

3. The system of claim 1 or 2, wherein the authorizing device is controlled by a judge and the root block further comprises a cryptographic key associated with the judge.

4. The system of claim 1, 2, or 3, wherein the root block further comprises access parameters to the data repository.

5. The system of claim 4, wherein the access parameters include one of an access duration, an identification of content to be accessed, or identification of an authorized accessor.

6. The system of any preceding claim, wherein the accessing device is controlled by a law enforcement agency and the digital authorization provides the access right of the law enforcement agency to the data repository.

7. The system of any preceding claim, wherein the administration service comprises one of a user plane function (UPF), session management function (SMF), or access and mobility management function (AMF).

8. A method for managing access to a data repository, the method comprising:

receiving, at a blockchain service node of a plurality of blockchain service nodes and from an authorizing device over a network, a root block comprising a digital authorization for accessing data stored in a data repository and an identification of the data repository;

receiving, at a master node and from the service node, the root block, the master node storing a consensus protocol defining a network consensus requirement for access to the data repository pursuant to the digital authorization stored at the blockchain service node;

transmitting, from the master node and to the plurality of blockchain service nodes, the root block;

receiving, at the master node and from an accessing device, a request to access the data repository;

verifying, by a portion of the plurality of blockchain service nodes and according to the consensus protocol, an access right to the data repository, the access right associated with the accessing device and digital authorization;

generating, by the master node, a record of access to the data repository by the accessing device, the record of access including a reference to the root block either directly or indirectly through at least one other record including a reference to the root block; and

storing, by the master node, the record of access.

9. The method of claim 8, wherein the consensus protocol comprises identification of a portion of the plurality of blockchain nodes for verifying an access right to the data repository and the method further comprising:

transmitting, from the master node and to the portion of the plurality of blockchain service nodes, the consensus protocol.

10. The method of claim 8 or 9, wherein the master node indirectly receives from the accessing device the request to access the data repository through one of the service node or a second service node of the plurality of blockchain service nodes.

11. The method of claim 8, 9, or 10, further comprising storing, by each service node of the plurality of service nodes, a copy of the record of access.

12. The method of any of claims 8 to 11, wherein the authorizing device is controlled by a judge and the root block further comprises a cryptographic key associated with the judge.

13. The method of any of claims 8 to 12, wherein the root block further comprises access parameters to the data repository.

14. The method of claim 13, wherein the access parameters include one of an access duration, an identification of content to be accessed, or an identification of an authorized accessor.

15. The method of any of claims 8 to 14, wherein the accessing device is controlled by a law enforcement agency and the digital authorization provides the access right of the law enforcement agency to the data repository.

16. The method of any of claims 8 to 15, wherein the network comprises an administration service, the administration service comprising one of a user plane function (UPF), a session management function (SMF), or an access and mobility management function (AMF).

17. At least one non-transitory computer readable medium comprising instructions stored thereon, the instructions effective to cause one or more network connected devices to:

receive, at a blockchain service node of a plurality of blockchain service nodes and from an authorizing device over a network, a root block comprising a digital authorization for accessing data stored in a data repository and an identification of the data repository;

receive, at a master node and from the service node, the root block, the master node storing a consensus protocol defining a network consensus requirement for access to the data repository pursuant to the digital authorization stored at the blockchain service node, the consensus protocol comprising identification of a portion of the plurality of blockchain nodes for verifying an access right to the data repository;

transmit, from the master node and to the plurality of blockchain service nodes, the root block;

receive, at the master node and from an accessing device via one of the service node or a second service node of the plurality of blockchain service nodes, a request to access the data repository;

transmit, from the master node and to the portion of the plurality of blockchain service nodes, the consensus protocol;

verify, by the portion of the plurality of blockchain service nodes and according to the consensus protocol, an access right to the data repository, the access right associated with the accessing device and digital authorization;

generate, by the master node, a record of access to the data repository by the accessing device, the record of access including a reference to the root block either directly or indirectly through at least one other record including a reference to the root block;

store, by the master node, the record of access; and

store, by each service node of the plurality of service nodes, a copy of the record of access.

18. The non-transitory computer readable medium of claim 17, wherein the authorizing device is controlled by a judge and the root block further comprises a cryptographic key associated with the judge.

19. The non-transitory computer readable medium of claim 17 or 18, wherein the accessing device is controlled by a law enforcement agency and the digital authorization provides the access right of the law enforcement agency to the data repository.

20. The non-transitory computer readable medium of claim 17, 18, or 19, wherein the network comprising an administration service, the administration service comprising one of a user plane function (UPF), a session management function (SMF), or an access and mobility management function (AMF).

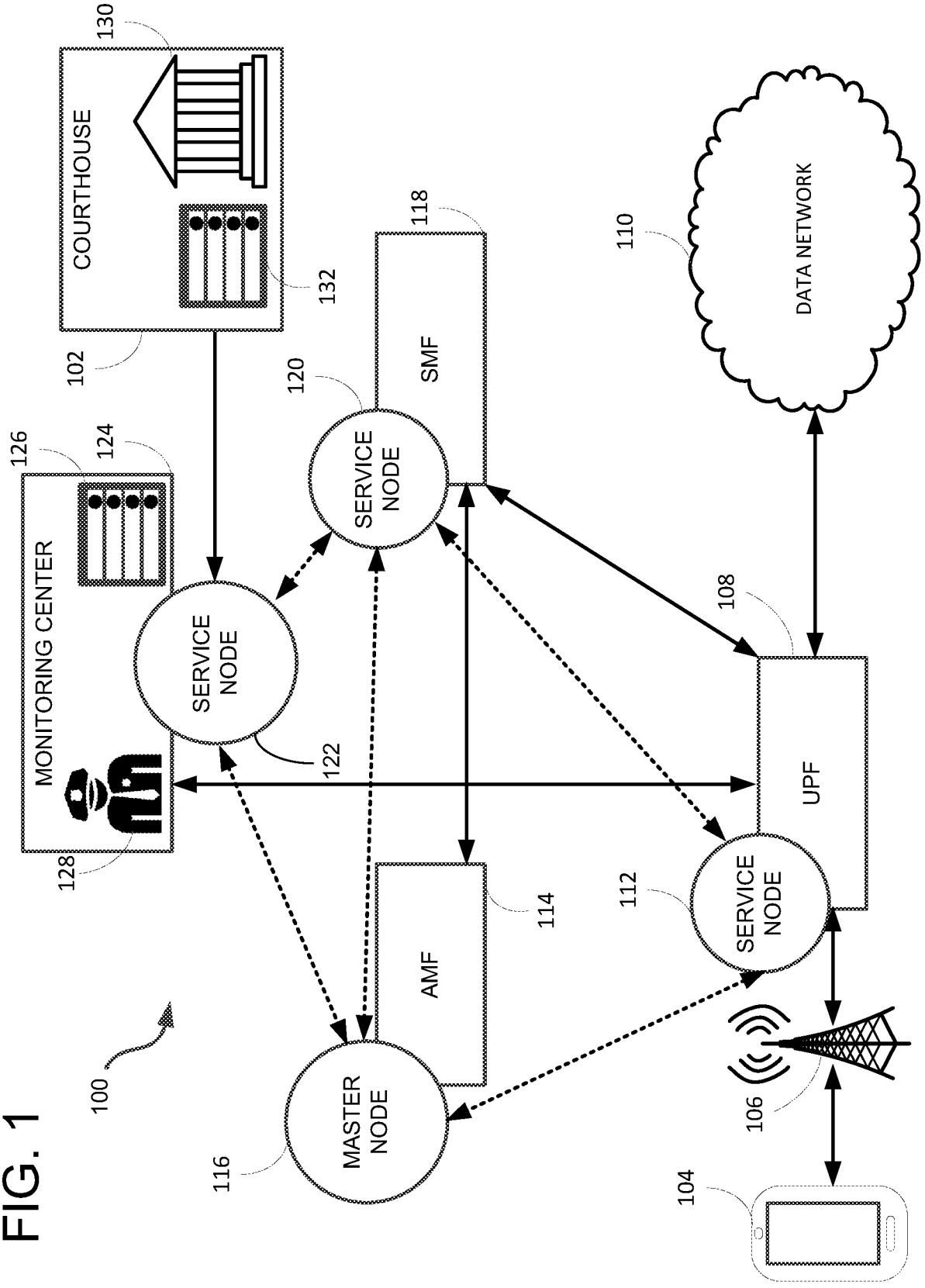

COURTHOUSE
130
132
102
MONITORING CENTER
126
124
128
SERVICE NODE
122
SERVICE NODE
120
SMF
118
DATA NETWORK
110
108
UPF
SERVICE NODE
112
AMF
114
MASTER NODE
116
100
106
104

FIG. 1

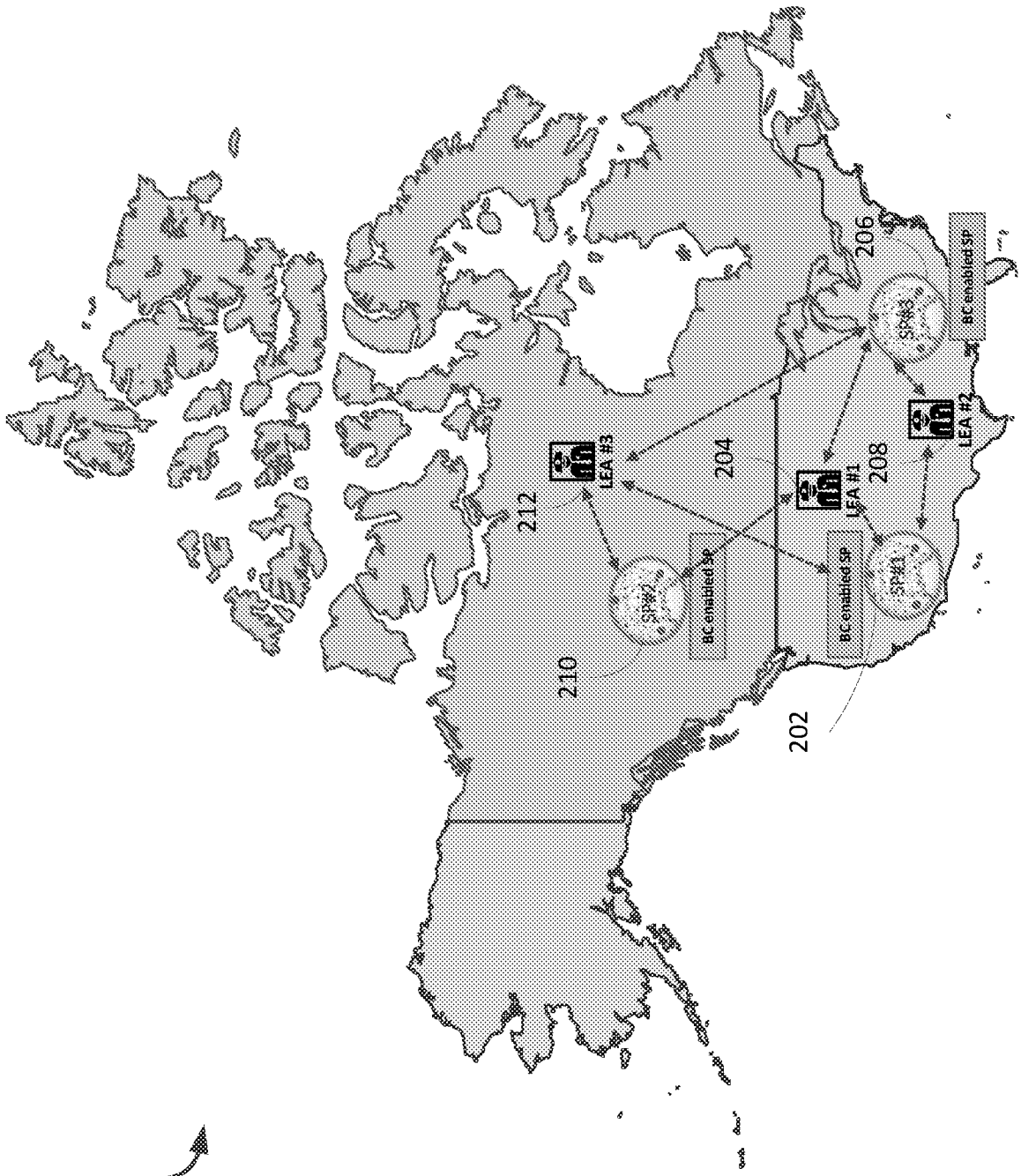

200
202
204
206
208
210
212
LEA #1
LEA #2
LEA #3
SP#1
SP#2
SP#3
BC enabled SP
BC enabled SP
BC enabled SP

FIG. 2

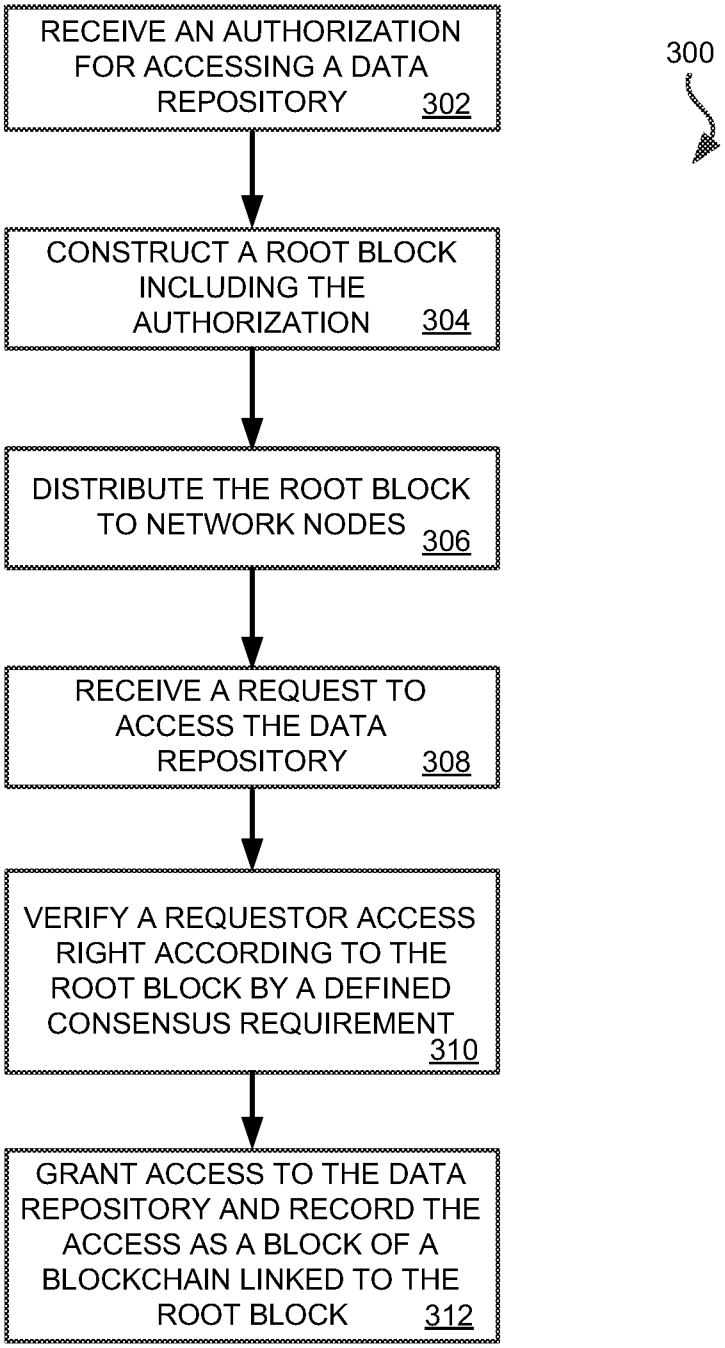

RECEIVE AN AUTHORIZATION FOR ACCESSING A DATA REPOSITORY 302
300
CONSTRUCT A ROOT BLOCK INCLUDING THE AUTHORIZATION 304
DISTRIBUTE THE ROOT BLOCK TO NETWORK NODES 306
RECEIVE A REQUEST TO ACCESS THE DATA REPOSITORY 308
VERIFY A REQUESTOR ACCESS RIGHT ACCORDING TO THE ROOT BLOCK BY A DEFINED CONSENSUS REQUIREMENT 310
GRANT ACCESS TO THE DATA REPOSITORY AND RECORD THE ACCESS AS A BLOCK OF A BLOCKCHAIN LINKED TO THE ROOT BLOCK 312

FIG. 3

FIG. 4

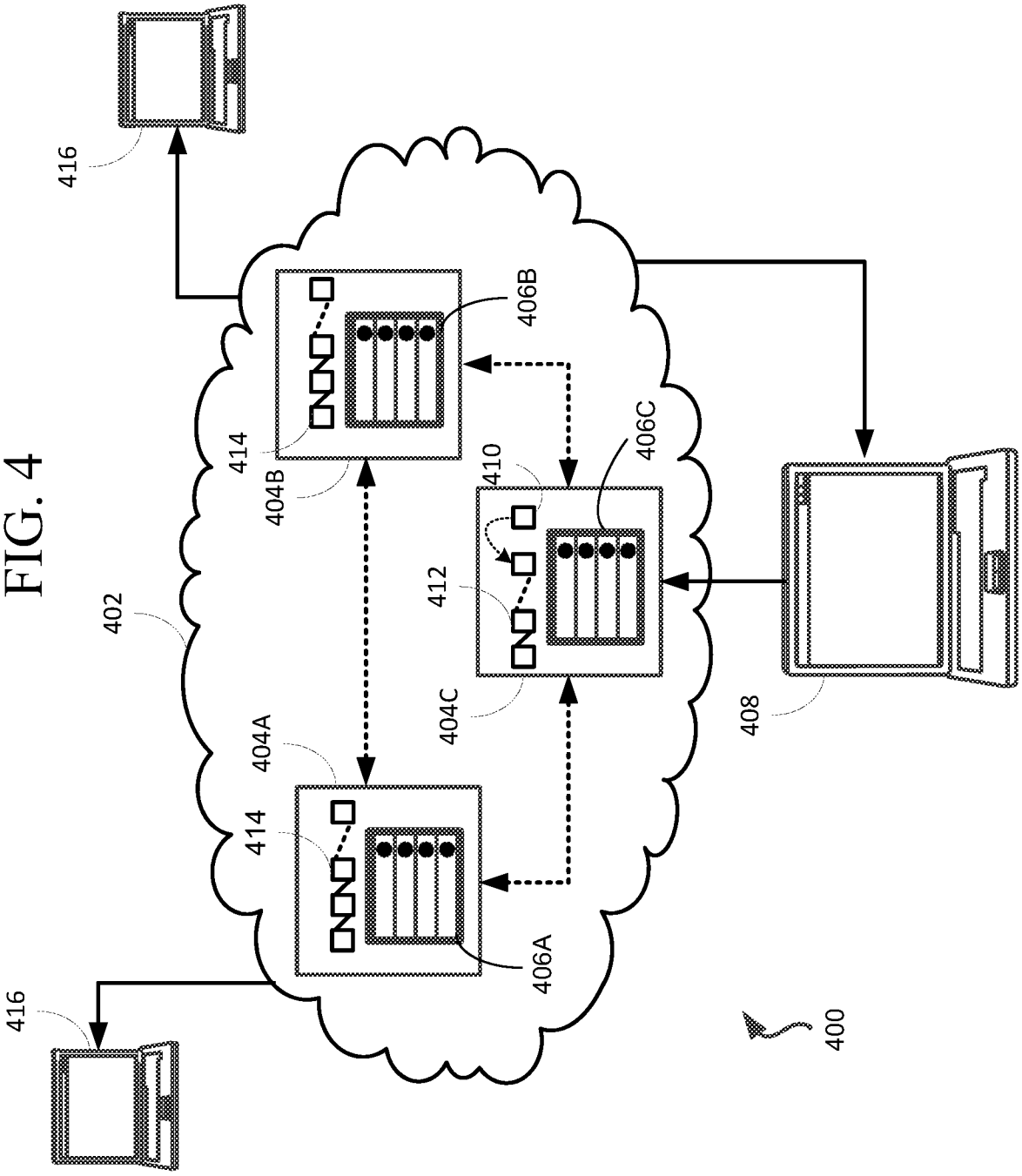

416
406B
414
404B
410
406C
412
402
404C
408
404A
414
406A
416
400

FIG. 5

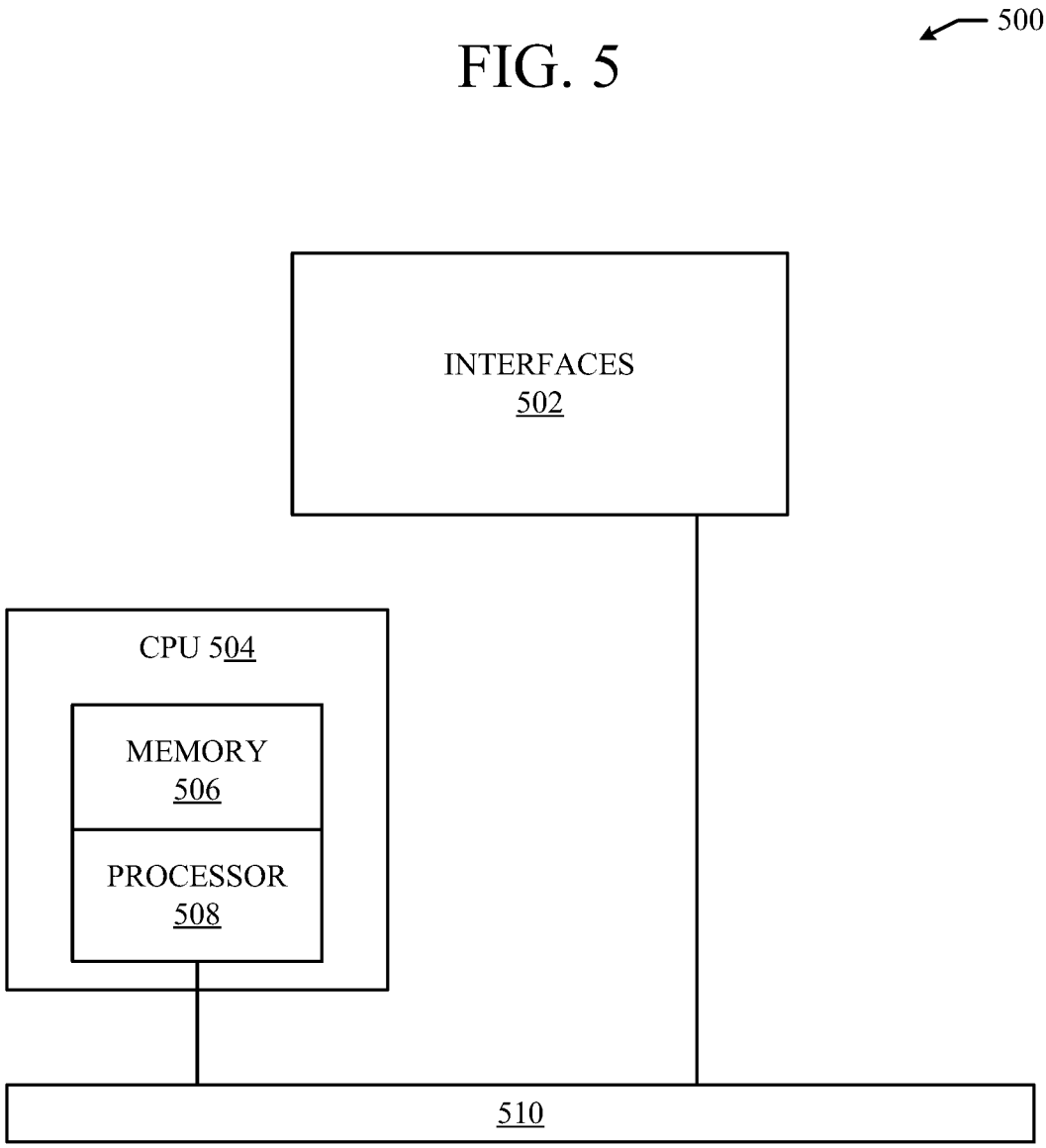
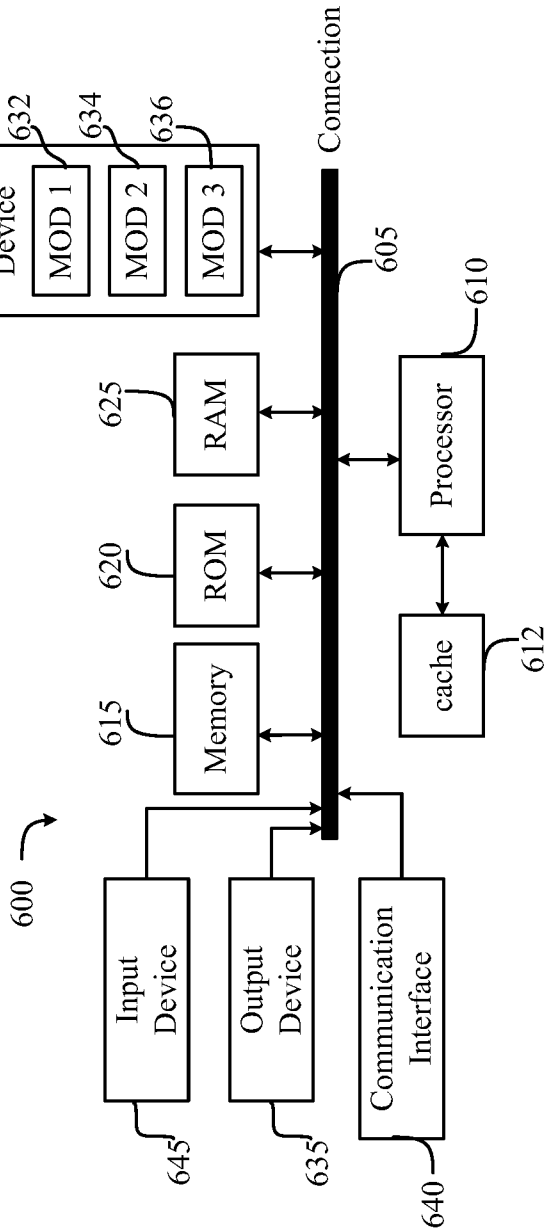


FIG. 6


600
Input Device
645
Output Device
635
Communication Interface
640
Memory
615
ROM
620
RAM
625
Storage Device
630
MOD 1
632
MOD 2
634
MOD 3
636
Connection
605
Processor
610
cache
612

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2018/045682

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - G06F 21/62; H04L 9/32; G06F 17/30; H04L 29/06 (2018.01)

CPC - H04L 9/0637; H04L 9/3236; H04L 9/3247; G06F 17/30371; G06F 21/6245; G06F 21/64; G06Q 20/3827 (2018.08)

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

See Search History document

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

USPC - 705/44; 455/410; 726/5 (keyword delimited)

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

See Search History document

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | US 2017/0346830 A1 (ALTR SOLUTIONS, INC.) 30 November 2017 (30.11.2017) entire document | 1-3, 8-10, 17-19 |
| A | US 2017/0287090 A1 (CLAUSE, INC.) 05 October 2017 (05.10.2017) entire document | 1-3, 8-10, 17-19 |
| A | PATEL et al. Blockchain Exhumed. IEEE. 2017. [retrieved on 2018-09-25]. Retrieved from the Internet:<URL:https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7976993>. entire document. | 1-3, 8-10, 17-19 |
| A | ORTIGOSA. Secure Code Distribution based on BlockChain. Distribution De C´odigo Seguro, VOL. 1, NO. 1. December 2016. [retrieved on 2018-09-25]. Retrieved from the Internet:<URL: https://pdfs.semanticscholar.org/0038/62907f294e72d8c12bd0d0e965f91da342f5.pdf>. entire document. | 1-3, 8-10, 17-19 |
| A | US 2017/0228822 A1 (DOMUS TOWER, INC.) 10 August 2017 (10.08.2017) entire document | 1-3, 8-10, 17-19 |
| A | US 2015/0244690 A1 (ENT TECHNOLOGIES, INC.) 27 August 2015 (27.08.2015) entire document | 1-3, 8-10, 17-19 |
| A | US 2017/0075941 A1 (FINLOW-BATES) 16 March 2017 (16.03.2017) entire document | 1-3, 8-10, 17-19 |
| A | WO 2017/204943 A1 (MASTERCARD INTERNATIONAL INCORPORATED) 30 November 2017 (30.11.2017) entire document | 1-3, 8-10, 17-19 |

☐ 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 |
|---|---|
| 25 September 2018 | 11 DEC 2018 |
| Name and mailing address of the ISA/US<br>Mail Stop PCT, Attn: ISA/US, Commissioner for Patents<br>P.O. Box 1450, Alexandria, VA 22313-1450<br>Facsimile No. 571-273-8300 | Authorized officer<br>Blaine R. Copenheaver<br>PCT Helpdesk: 571-272-4300<br>PCT OSP: 571-272-7774 |

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2018/045682

**Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)**

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☒ Claims Nos.: 4-7, 11-16, 20
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

**Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)**

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

**Remark on Protest**

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.