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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
03 December 2020 (03.12.2020)

WIPO | PCT

(10) International Publication Number
WO 2020/242584 A1

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

(21) International Application Number:
PCT/US2020/026030

(22) International Filing Date:
31 March 2020 (31.03.2020)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
16/425,608 29 May 2019 (29.05.2019) US

(71) Applicant: **MICROSOFT TECHNOLOGY LICENSING, LLC** [US/US]; One Microsoft Way, Redmond, Washington 98052-6399 (US).

(72) Inventors: **MURDOCH, Brandon**; MICROSOFT TECHNOLOGY LICENSING, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US). **PATEL, Ankur**; MICROSOFT TECHNOLOGY LICENSING, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US). **CHIACHIERE, Frank Michael**; MICROSOFT TECHNOLOGY LICENSING, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US). **BERCIK, Bailey Marie**; MICROSOFT TECHNOLOGY LICENSING, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US).

(74) Agent: **SWAIN, Cassandra T.** et al.; MICROSOFT TECHNOLOGY LICENSING, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (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,

(54) Title: DYNAMIC GENERATION OF PSEUDONYMOUS NAMES

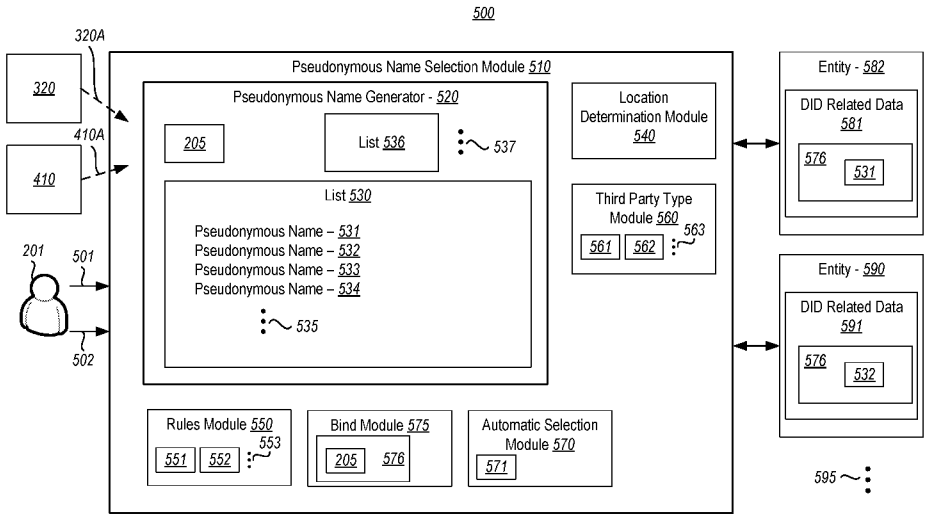


FIG. 5

(57) Abstract: Embodiments disclosed herein are related to computing systems and methods for generating one or more pseudonymous names for use by a Decentralized Identifier (DID) owner when interacting with third party entities. An indication is received from a DID owner who is associated with a DID. The indication indicates that the DID owner desires to interact with various third party entities. A list is generated of pseudonymous names that are to be used in place of the DID as the DID owner interacts with the one or more third party entities. A selection is received for a specific one of the generated pseudonymous names. The selected specific pseudonymous name is bound to the DID so that the selected specific pseudonymous name is used during the interaction.

WO 2020/242584 A1

[Continued on next page]

MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

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

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))*

DYNAMIC GENERATION OF PSEUDONYMOUS NAMES

BACKGROUND

[0001] Most currently used documents or records that prove identity are issued by centralized organizations, such as governments, schools, employers, or other service centers or regulatory organizations. These organizations often maintain every member's identity in a centralized identity management system. A centralized identity management system is a centralized information system used for organizations to manage the issued identities, their authentication, authorization, roles and privileges. Centralized identity management systems have been deemed as secure since they often use professionally maintained hardware and software. Typically, the identity issuing organization sets the terms and requirements for registering people with the organization. When a party needs to verify another party's identity, the verifying party often needs to go through the centralized identity management system to obtain information verifying and/or authenticating the other party's identity.

[0002] Decentralized Identifiers (DIDs) are a new type of identifier, which are independent from any centralized registry, identity provider, or certificate authority. Distributed ledger technology (such as blockchain) provides the opportunity for using fully decentralized identifiers. Distributed ledger technology uses globally distributed ledgers to record transactions between two or more parties in a verifiable way. Once a transaction is recorded, the data in the section of ledger cannot be altered retroactively without the alteration of all subsequent sections of ledger, which provides a fairly secure platform. Since a DID is generally not controlled by a centralized management system but rather is owned by an owner of the DID, DIDs are sometimes referred to as identities without authority.

[0003] The subject matter claimed herein is not limited to embodiments that solve any disadvantages or that operate only in environments such as those described above. Rather, this background is only provided to illustrate one exemplary technology area where some embodiments describe herein may be practiced.

BRIEF SUMMARY

[0004] This Summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description. This Summary is not intended to identify key features or essential features of the claimed subject matter, nor is it intended to be used as an aid in determining the scope of the claimed subject matter.

[0005] Embodiments disclosed herein are related to computing systems and methods

for generating one or more pseudonymous names for use by a Decentralized Identifier (DID) owner when interacting with third party entities. An indication is received from a DID owner who is associated with a DID. The indication indicates that the DID owner desires to interact with various third party entities. A list is generated of pseudonymous names that are to be used in place of the DID as the DID owner interacts with the one or more third party entities. A selection is received for a specific one of the generated pseudonymous names. The selected specific pseudonymous name is bound to the DID so that the selected specific pseudonymous name is used during the interaction.

[0006] Additional features and advantages will be set forth in the description which follows, and in part will be obvious from the description, or may be learned by the practice of the teachings herein. Features and advantages of the invention may be realized and obtained by means of the instruments and combinations particularly pointed out in the appended claims. Features of the present invention will become more fully apparent from the following description and appended claims, or may be learned by the practice of the invention as set forth hereinafter.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] In order to describe the manner in which the above-recited and other advantages and features can be obtained, a more particular description of the subject matter briefly described above will be rendered by reference to specific embodiments which are illustrated in the appended drawings. Understanding that these drawings depict only typical embodiments and are not therefore to be considered to be limiting in scope, embodiments will be described and explained with additional specificity and details through the use of the accompanying drawings in which:

[0008] Figure 1 illustrates an example computing system in which the principles described herein may be employed;

[0009] Figure 2 illustrates an example environment for creating a decentralized identification (DID);

[0010] Figure 3 illustrates an example environment for various DID management operations and services;

[0011] Figure 4 illustrates an example decentralized storage device or identity hubs;

[0012] Figure 5 illustrates an example embodiment of an environment for generating pseudonymous names for use in interactions with third party entities; and

[0013] Figure 6 illustrates a flow chart of an example method for generating pseudonymous names for use in interactions with third party entities.

DETAILED DESCRIPTION

[0014] Embodiments disclosed herein are related to computing systems and methods for generating one or more pseudonymous names for use by a Decentralized Identifier (DID) owner when interacting with third party entities. An indication is received from a DID owner who is associated with a DID. The indication indicates that the DID owner desires to interact with various third party entities. A list is generated of pseudonymous names that are to be used in place of the DID as the DID owner interacts with the one or more third party entities. A selection is received for a specific one of the generated pseudonymous names. The selected specific pseudonymous name is bound to the DID so that the selected specific pseudonymous name is used during the interaction.

[0015] The embodiments disclosed herein represent a technical advance over existing systems. For example, a DID is often used as an identifier for a DID owner during interactions with a third party entity. For instance, the DID may be used to show the identity of the DID owner when he or she makes a public comment on a blog post or the like. Although allowing public access to the DID may not cause the actual identity of the DID owner to become known, there may still be security and privacy issues with such public disclosure. Accordingly, the DID owner may desire to use a different identifier in place of the DID

[0016] The embodiments disclosed herein provide a way to generate various pseudonymous name that may be bound to the DID. The pseudonymous names may then be used in place of the DID during interactions with the third party entities. For example, in the case of the comment on the blog entry the DID owner 201 may use a pseudonymous name instead of the DID as an identifier when making the comment. In this way the DID owner is able to achieve increased security and privacy since the DID itself is not shown in the comments section of the blog. However, since the DID is bound to the pseudonymous name the advantages provided by having a DID tied to a decentralized network are still available to the DID owner.

[0017] Because the principles described herein may be performed in the context of a computing system, some introductory discussion of a computing system will be described with respect to Figure 1. Then, this description will return to the principles of a decentralized identifier (DID) platform with respect to the remaining figures.

[0018] Computing systems are now increasingly taking a wide variety of forms. Computing systems may, for example, be handheld devices, appliances, laptop computers, desktop computers, mainframes, distributed computing systems, data centers, or even

devices that have not conventionally been considered a computing system, such as wearables (e.g., glasses). In this description and in the claims, the term "computing system" is defined broadly as including any device or system (or a combination thereof) that includes at least one physical and tangible processor, and a physical and tangible memory capable of having thereon computer-executable instructions that may be executed by a processor. The memory may take any form and may depend on the nature and form of the computing system. A computing system may be distributed over a network environment and may include multiple constituent computing systems.

[0019] As illustrated in Figure 1, in its most basic configuration, a computing system 100 typically includes at least one hardware processing unit 102 and memory 104. The processing unit 102 may include a general-purpose processor and may also include a field programmable gate array (FPGA), an application specific integrated circuit (ASIC), or any other specialized circuit. The memory 104 may be physical system memory, which may be volatile, non-volatile, or some combination of the two. The term "memory" may also be used herein to refer to non-volatile mass storage such as physical storage media. If the computing system is distributed, the processing, memory and/or storage capability may be distributed as well.

[0020] The computing system 100 also has thereon multiple structures often referred to as an "executable component". For instance, the memory 104 of the computing system 100 is illustrated as including executable component 106. The term "executable component" is the name for a structure that is well understood to one of ordinary skill in the art in the field of computing as being a structure that can be software, hardware, or a combination thereof. For instance, when implemented in software, one of ordinary skill in the art would understand that the structure of an executable component may include software objects, routines, methods, and so forth, that may be executed on the computing system, whether such an executable component exists in the heap of a computing system, or whether the executable component exists on computer-readable storage media.

[0021] In such a case, one of ordinary skill in the art will recognize that the structure of the executable component exists on a computer-readable medium such that, when interpreted by one or more processors of a computing system (e.g., by a processor thread), the computing system is caused to perform a function. Such structure may be computer readable directly by the processors (as is the case if the executable component were binary). Alternatively, the structure may be structured to be interpretable and/or compiled (whether in a single stage or in multiple stages) so as to generate such binary that is directly

interpretable by the processors. Such an understanding of example structures of an executable component is well within the understanding of one of ordinary skill in the art of computing when using the term "executable component".

[0022] The term "executable component" is also well understood by one of ordinary skill as including structures, such as hard coded or hard wired logic gates, that are implemented exclusively or near-exclusively in hardware, such as within a field programmable gate array (FPGA), an application specific integrated circuit (ASIC), or any other specialized circuit. Accordingly, the term "executable component" is a term for a structure that is well understood by those of ordinary skill in the art of computing, whether implemented in software, hardware, or a combination. In this description, the terms "component", "agent", "manager", "service", "engine", "module", "virtual machine" or the like may also be used. As used in this description and in the case, these terms (whether expressed with or without a modifying clause) are also intended to be synonymous with the term "executable component", and thus also have a structure that is well understood by those of ordinary skill in the art of computing.

[0023] In the description that follows, embodiments are described with reference to acts that are performed by one or more computing systems. If such acts are implemented in software, one or more processors (of the associated computing system that performs the act) direct the operation of the computing system in response to having executed computer-executable instructions that constitute an executable component. For example, such computer-executable instructions may be embodied on one or more computer-readable media that form a computer program product. An example of such an operation involves the manipulation of data. If such acts are implemented exclusively or near-exclusively in hardware, such as within a FPGA or an ASIC, the computer-executable instructions may be hard-coded or hard-wired logic gates. The computer-executable instructions (and the manipulated data) may be stored in the memory 104 of the computing system 100. Computing system 100 may also contain communication channels 108 that allow the computing system 100 to communicate with other computing systems over, for example, network 110.

[0024] While not all computing systems require a user interface, in some embodiments, the computing system 100 includes a user interface system 112 for use in interfacing with a user. The user interface system 112 may include output mechanisms 112A as well as input mechanisms 112B. The principles described herein are not limited to the precise output mechanisms 112A or input mechanisms 112B as such will depend on the nature of the

device. However, output mechanisms 112A might include, for instance, speakers, displays, tactile output, virtual or augmented reality, holograms and so forth. Examples of input mechanisms 112B might include, for instance, microphones, touchscreens, virtual or augmented reality, holograms, cameras, keyboards, mouse or other pointer input, sensors of any type, and so forth.

[0025] Embodiments described herein may comprise or utilize a special-purpose or general-purpose computing system including computer hardware, such as, for example, one or more processors and system memory, as discussed in greater detail below. Embodiments described herein also include physical and other computer-readable media for carrying or storing computer-executable instructions and/or data structures. Such computer-readable media can be any available media that can be accessed by a general-purpose or special-purpose computing system. Computer-readable media that store computer-executable instructions are physical storage media. Computer-readable media that carry computer-executable instructions are transmission media. Thus, by way of example, and not limitation, embodiments of the invention can comprise at least two distinctly different kinds of computer-readable media: storage media and transmission media.

[0026] Computer-readable storage media includes RAM, ROM, EEPROM, CD-ROM, or other optical disk storage, magnetic disk storage, or other magnetic storage devices, or any other physical and tangible storage medium which can be used to store desired program code means in the form of computer-executable instructions or data structures and which can be accessed by a general-purpose or special-purpose computing system.

[0027] A "network" is defined as one or more data links that enable the transport of electronic data between computing systems and/or modules and/or other electronic devices. When information is transferred or provided over a network or another communications connection (either hardwired, wireless, or a combination of hardwired or wireless) to a computing system, the computing system properly views the connection as a transmission medium. Transmission media can include a network and/or data links which can be used to carry desired program code means in the form of computer-executable instructions or data structures and which can be accessed by a general-purpose or special-purpose computing system. Combinations of the above should also be included within the scope of computer-readable media.

[0028] Further, upon reaching various computing system components, program code means in the form of computer-executable instructions or data structures can be transferred automatically from transmission media to storage media (or vice versa). For example,

computer-executable instructions or data structures received over a network or data link can be buffered in RAM within a network interface module (e.g., a "NIC"), and then be eventually transferred to computing system RAM and/or to less volatile storage media at a computing system. Thus, it should be understood that storage media can be included in computing system components that also (or even primarily) utilize transmission media.

[0029] Computer-executable instructions comprise, for example, instructions and data which, when executed at a processor, cause a general-purpose computing system, special-purpose computing system, or special-purpose processing device to perform a certain function or group of functions. Alternatively, or in addition, the computer-executable instructions may configure the computing system to perform a certain function or group of functions. The computer executable instructions may be, for example, binaries or even instructions that undergo some translation (such as compilation) before direct execution by the processors, such as intermediate format instructions such as assembly language, or even source code.

[0030] Although the subject matter has been described in language specific to structural features and/or methodological acts, it is to be understood that the subject matter defined in the appended claims is not necessarily limited to the described features or acts described above. Rather, the described features and acts are disclosed as example forms of implementing the claims.

[0031] Those skilled in the art will appreciate that the invention may be practiced in network computing environments with many types of computing system configurations, including, personal computers, desktop computers, laptop computers, message processors, hand-held devices, multi-processor systems, microprocessor-based or programmable consumer electronics, network PCs, minicomputers, mainframe computers, mobile telephones, PDAs, pagers, routers, switches, datacenters, wearables (such as glasses) and the like. The invention may also be practiced in distributed system environments where local and remote computing system, which are linked (either by hardwired data links, wireless data links, or by a combination of hardwired and wireless data links) through a network, both perform tasks. In a distributed system environment, program modules may be located in both local and remote memory storage devices.

[0032] Those skilled in the art will also appreciate that the invention may be practiced in a cloud computing environment. Cloud computing environments may be distributed, although this is not required. When distributed, cloud computing environments may be distributed internationally within an organization and/or have components possessed across

multiple organizations. In this description and the following claims, "cloud computing" is defined as a model for enabling on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services). The definition of "cloud computing" is not limited to any of the other numerous advantages that can be obtained from such a model when properly deployed.

[0033] The remaining figures may discuss various computing system which may correspond to the computing system 100 previously described. The computing systems of the remaining figures include various components or functional blocks that may implement the various embodiments disclosed herein as will be explained. The various components or functional blocks may be implemented on a local computing system or may be implemented on a distributed computing system that includes elements resident in the cloud or that implement aspects of cloud computing. The various components or functional blocks may be implemented as software, hardware, or a combination of software and hardware. The computing systems of the remaining figures may include more or less than the components illustrated in the figures and some of the components may be combined as circumstances warrant.

[0034] Some introductory discussion of a decentralized identifier (DID) and the environment in which they are created and reside will now be given with respect to Figure 2. As illustrated in Figure 2, a DID owner 201 may own or control a DID 205 that represents an identity of the DID owner 201. The DID owner 201 may register a DID using a creation and registration service, which will be explained in more detail below.

[0035] The DID owner 201 may be any entity that could benefit from a DID. For example, the DID owner 201 may be a human being or an organization of human beings. Such organizations might include a company, department, government, agency, or any other organization or group of organizations. Each individual human being might have a DID while the organization(s) to which each belongs might likewise have a DID.

[0036] The DID owner 201 may alternatively be a machine, system, or device, or a collection of machine(s), device(s) and/or system(s). In still other embodiments, the DID owner 201 may be a subpart of a machine, system or device. For instance, a device could be a printed circuit board, where the subpart of that circuit board are individual components of the circuit board. In such embodiments, the machine or device may have a DID and each subpart may also have a DID. A DID owner might also be a software component such as the executable component 106 described above with respect to Figure 1. An example of a complex executable component 106 might be an artificial intelligence. Accordingly, an

artificial intelligence may also own a DID.

[0037] Thus, the DID owner 201 may be any entity, human or non-human, that is capable of creating the DID 205 or at least having the DID 205 created for and/or associated with them. Although the DID owner 201 is shown as having a single DID 205, this need not be the case as there may be any number of DIDs associated with the DID owner 201 as circumstances warrant.

[0038] As mentioned, the DID owner 201 may create and register the DID 205. The DID 205 may be any identifier that may be associated with the DID owner 201. Preferably, that identifier is unique to that DID owner 201, at least within a scope in which the DID is anticipated to be in use. As an example, the identifier may be a locally unique identifier, and perhaps more desirably a globally unique identifier for identity systems anticipated to operate globally. In some embodiments, the DID 205 may be a Uniform Resource identifier (URI) (such as a Uniform Resource Locator (URL)) or other pointer that relates the DID owner 201 to mechanisms to engage in trustable interactions with the DID owner 201.

[0039] The DID 205 is "decentralized" because it does not require a centralized, third party management system for generation, management, or use. Accordingly, the DID 205 remains under the control of the DID owner 201. This is different from conventional centralized IDs which base trust on centralized authorities and that remain under control of corporate directory services, certificate authorities, domain name registries, or other centralized authority (referred to collectively as "centralized authorities" herein). Accordingly, the DID 205 may be any identifier that is under the control of the DID owner 201 and that is independent of any centralized authority.

[0040] In some embodiments, the structure of the DID 205 may be as simple as a user name or some other human-understandable term. However, in other embodiments, for increased security, the DID 205 may preferably be a random string of numbers and letters. In one embodiment, the DID 205 may be a string of 128 numbers and letters. Accordingly, the embodiments disclosed herein are not dependent on any specific implementation of the DID 205. In a very simple example, the DID 205 is shown within the figures as "123ABC".

[0041] As also shown in Figure 2, the DID owner 201 has control of a private key 206 and public key 207 pair that is associated with the DID 205. Because the DID 205 is independent of any centralized authority, the private key 206 should at all times be fully in control of the DID owner 201. That is, the private and public keys should be generated in a decentralized manner that ensures that they remain under the control of the DID owner 201.

[0042] As will be described in more detail to follow, the private key 206 and public key

207 pair may be generated on a device controlled by the DID owner 201. The private key 206 and public key 207 pair should not be generated on a server controlled by any centralized authority as this may cause the private key 206 and public key 207 pair to not be fully under the control of the DID owner 201 at all times. Although figure 2 and this description have described a private and public key pair, it will also be noted that other types of reasonable cryptographic information and/or mechanisms may also be used as circumstances warrant.

[0043] Figure 2 also illustrates a DID document 210 that is associated with the DID 205. As will be explained in more detail to follow, the DID document 210 may be generated at the time that the DID 205 is created. In its simplest form, the DID document 210 describes how to use the DID 205. Accordingly, the DID document 210 includes a reference to the DID 205, which is the DID that is described by the DID document 210. In some embodiments, the DID document 210 may be implemented according to methods specified by a distributed ledger 220 (such as blockchain) that will be used to store a representation of the DID 205 as will be explained in more detail to follow. Thus, the DID document 210 may have different methods depending on the specific distributed ledger.

[0044] The DID document 210 also includes the public key 207 created by the DID owner 201 or some other equivalent cryptographic information. The public key 207 may be used by third party entities that are given permission by the DID owner 201 to access information and data owned by the DID owner 201. The public key 207 may also be used to verify that the DID owner 201 in fact owns or controls the DID 205.

[0045] The DID document 210 may also include authentication information 211. The authentication information 211 may specify one or more mechanisms by which the DID owner 201 is able to prove that the DID owner 201 owns the DID 205. In other words, the mechanisms of the authentication information 211 may show proof of a binding between the DID 205 (and thus its DID owner 201) and the DID document 210. In one embodiment, the authentication information 211 may specify that the public key 207 be used in a signature operation to prove the ownership of the DID 205. Alternatively, or in addition, the authentication information 211 may specify that the public key 207 be used in a biometric operation to prove ownership of the DID 205. Accordingly, the authentication information 211 may include any number of mechanisms by which the DID owner 201 is able to prove that the DID owner 201 owns the DID 205.

[0046] The DID document 210 may also include authorization information 212. The authorization information 212 may allow the DID owner 201 to authorize third party entities

the rights to modify the DID document 210 or some part of the document without giving the third party the right to prove ownership of the DID 205. For example, the authorization information 212 may allow the third party to update any designated set of one or more fields in the DID document 210 using any designated update mechanism. Alternatively, the authorization information may allow the third party to limit the usages of DID 205 by the DID owner 201 for a specified time period. This may be useful when the DID owner 201 is a minor child and the third party is a parent or guardian of the child. The authorization information 212 may allow the parent or guardian to limit use of the DID owner 201 until such time as the child is no longer a minor.

[0047] The authorization information 212 may also specify one or more mechanisms that the third party will need to follow to prove they are authorized to modify the DID document 210. In some embodiments, these mechanisms may be similar to those discussed previously with respect to the authentication information 211.

[0048] The DID document 210 may also include one or more service endpoints 213. A service endpoint may include a network address at which a service operates on behalf of the DID owner 201. Examples of specific services include discovery services, social networks, file storage services such as identity servers or hubs, and verifiable claim repository services. Accordingly, the service endpoints 213 operate as pointers for the services that operate on behalf of the DID owner 201. These pointers may be used by the DID owner 201 or by third party entities to access the services that operate on behalf of the DID owner 201. Specific examples of service endpoints 213 will be explained in more detail to follow.

[0049] The DID document 210 may further include identification information 214. The identification information 214 may include personally identifiable information such as the name, address, occupation, family members, age, hobbies, interests, or the like of DID owner 201. Accordingly, the identification information 214 listed in the DID document 210 may represent a different persona of the DID owner 201 for different purposes.

[0050] A persona may be pseudo anonymous. As an example, the DID owner 201 may include a pen name in the DID document when identifying him or her as a writer posting articles on a blog. A persona may be fully anonymous. As an example, the DID owner 201 may only want to disclose his or her job title or other background data (e.g., a school teacher, an FBI agent, an adult older than 21 years old, etc.) but not his or her name in the DID document. As yet another example, a persona may be specific to who the DID owner 201 is as an individual. As an example, the DID owner 201 may include information identifying him or her as a volunteer for a particular charity organization, an employee of a particular

corporation, an award winner of a particular award, and so forth.

[0051] The DID document 210 may also include attestation information 215. The attestation information 215 may be any information that is associated with the DID owner 201's background. For instance, the attestation information 215 may be (but not limited to) a qualification, an achievement, a government ID, a government right such as a passport or a driver's license, a payment provider or bank account, a university degree or other educational history, employment status and history, or any other information about the DID owner 201's background. In some embodiments, the DID owner 201 collects various signed attestations that are included in the attestation information from different third party entities.

[0052] The DID document 210 may also include various other information 216. In some embodiments, the other information 216 may include metadata specifying when the DID document 210 was created and/or when it was last modified. In other embodiments, the other information 216 may include cryptographic proofs of the integrity of the DID document 210. In still further embodiments, the other information 216 may include additional information that is either specified by the specific method implementing the DID document or desired by the DID owner 201.

[0053] Figure 2 also illustrates a distributed ledger 220. The distributed ledger 220 may be any decentralized, distributed network that includes various computing systems that are in communication with each other. For example, the distributed ledger 220 may include a first distributed computing system 230, a second distributed computing system 240, a third distributed computing system 250, and any number of additional distributed computing systems as illustrated by the ellipses 260. The distributed ledger 220 may operate according to any known standards or methods for distributed ledgers. Examples of conventional distributed ledgers that may correspond to the distributed ledger 220 include, but are not limited to, Bitcoin [BTC], Ethereum, and Litecoin.

[0054] In the context of DID 205, the distributed ledger or blockchain 220 is used to store a representation of the DID 205 that points to the DID document 210. In some embodiments, the DID document 210 may be stored on the actual distributed ledger. Alternatively, in other embodiments the DID document 210 may be stored in a data storage (not illustrated) that is associated with the distributed ledger 220.

[0055] As mentioned, a representation of the DID 205 is stored on each distributed computing system of the distributed ledger 220. For example, in Figure 2 this is shown as DID hash 231, DID hash 241, and DID hash 251, which are ideally identical hashed copies of the same DID. The DID hash 231, DID hash 241, and DID hash 251 may then point to

the location of the DID document 210. The distributed ledger or blockchain 220 may also store numerous other representations of other DIDs as illustrated by references 232, 233, 234, 242, 243, 244, 252, 253, and 254.

[0056] In one embodiment, when the DID owner 201 creates the DID 205 and the associated DID document 210, the DID hash 231, DID hash 241, and DID hash 251 are written to the distributed ledger 220. The distributed ledger 220 thus records that the DID 205 now exists. Since the distributed ledger 220 is decentralized, the DID 205 is not under the control of any entity outside of the DID owner 201. DID hash 231, DID hash 241, and DID hash 251 may each include, in addition to the pointer to the DID document 210, a record or time stamp that specifies when the DID 205 was created. At a later date, when modifications are made to the DID document 210, each modification (and potentially also a timestamp of the modification) may also be recorded in DID hash 231, DID hash 241, and DID hash 251. DID hash 231, DID hash 241, and DID hash 251 may further include a copy of the public key 207 so that the DID 205 is cryptographically bound to the DID document 210.

[0057] Having described DIDs and how they operate generally with reference to Figure 2, specific embodiments of DID environments will now be explained. Turning to Figure 3, an environment 300 that may be used to perform various DID management operations and services will now be explained. It will be appreciated that the environment of Figure 3 may reference elements from Figure 2 as needed for ease of explanation.

[0058] As shown in Figure 3, the environment 300 may include various devices and computing systems that may be owned or otherwise under the control of the DID owner 201. These may include a user device 301. The user device 301 may be, but is not limited to, a mobile device such as a smart phone, a computing device such as a laptop computer, or any device such as a car or an appliance that includes computing abilities. The device 301 may include a web browser 302 operating on the device and an operating system 303 operating the device. More broadly speaking, the dashed line 304 represents that all of these devices may be owned or otherwise under the control of the DID owner 201.

[0059] The environment 300 also includes a DID management module 320. It will be noted that in operation, the DID management module 320 may reside on and be executed by one or more of user device 301, web browser 302, and the operating system 303 as illustrated by respective lines 301a, 302a, and 303a. Accordingly, the DID management module 320 is shown as being separate for ease of explanation. In some embodiments, the management module 320 may be referred to as a "digital wallet".

[0060] As shown in Figure 3, the DID management module 320 includes a DID creation module 330. The DID creation module 330 may be used by the DID owner 201 to create the DID 205 or any number of additional DIDs, such as DID 331. In one embodiment, the DID creation module may include or otherwise have access to a User Interface (UI) element 335 that may guide the DID owner 201 in creating the DID 205. The DID creation module 330 may have one or more drivers that are configured to work with specific distributed ledgers such as distributed ledger 220 so that the DID 205 complies with the underlying methods of that distributed ledger.

[0061] A specific embodiment will now be described. For example, the UI 335 may provide a prompt for the user to enter a user name or some other human recognizable name. This name may be used as a display name for the DID 205 that will be generated. As previously described, the DID 205 may be a long string of random numbers and letters and so having a human-recognizable name for a display name may be advantageous. The DID creation module 330 may then generate the DID 205. In the embodiments having the UI 335, the DID 205 may be shown in a listing of identities and may be associated with the human-recognizable name.

[0062] The DID creation module 330 may also include a key generation module 350. The key generation module may generate the private key 206 and public key 207 pair previously described. The DID creation module 330 may then use the DID 205 and the private and public key pair to generate the DID document 210.

[0063] In operation, the DID creation module 330 accesses a registrar 310 that is configured to the specific distributed ledger that will be recording the transactions related to the DID 205. The DID creation module 330 uses the registrar 310 to record DID hash 231, DID hash 241, and DID hash 251 in the distributed ledger in the manner previously described, and to store the DID document 210 in the manner previously described. This process may use the public key 207 in the hash generation.

[0064] In some embodiments, the DID management module 320 may include an ownership module 340. The ownership module 340 may provide mechanisms that ensure that the DID owner 201 is in sole control of the DID 205. In this way, the provider of the DID management module 320 is able to ensure that the provider does not control the DID 205, but is only providing the management services.

[0065] As previously discussed, the key generation module 350 generates the private key 206 and public key 207 pair and the public key 207 is then recorded in the DID document 210. Accordingly, the public key 207 may be used by all devices associated with

the DID owner 201 and all third parties that desire to provide services to the DID owner 201. Accordingly, when the DID owner 201 desires to associate a new device with the DID 205, the DID owner 201 may execute the DID creation module 330 on the new device. The DID creation module 330 may then use the registrar 310 to update the DID document 210 to reflect that the new device is now associated with the DID 205, which update would be reflected in a transaction on the distributed ledger 220, as previously described.

[0066] In some embodiments, however, it may be advantageous to have a public key per device 301 owned by the DID owner 201 as this may allow the DID owner 201 to sign with the device-specific public key without having to access a general public key. In other words, since the DID owner 201 will use different devices at different times (for example using a mobile phone in one instance and then using a laptop computer in another instance), it is advantageous to have a key associated with each device to provide efficiencies in signing using the keys. Accordingly, in such embodiments the key generation module 350 may generate additional public keys 208 and 209 when the additional devices execute the DID creation module 330. These additional public keys may be associated with the private key 206 or in some instances may be paired with a new private key.

[0067] In those embodiments where the additional public keys 208 and 209 are associated with different devices, the additional public keys 208 and 209 may be recorded in the DID document 210 as being associated with those devices. This is shown in Figure 3. It will be appreciated that the DID document 210 may include the information (information 205, 207 and 211 through 216) previously described in relation to Figure 2 in addition to the information (information 208, 209 and 365) shown in Figure 3. If the DID document 210 existed prior to the device-specific public keys being generated, then the DID document 210 would be updated by the creation module 330 via the registrar 310 and this would be reflected in an updated transaction on the distributed ledger 220.

[0068] In some embodiments, the DID owner 201 may desire to keep secret the association of a device with a public key or the association of a device with the DID 205. Accordingly, the DID creation module 330 may cause that such data be secretly shown in the DID document 210.

[0069] As described thus far, the DID 205 has been associated with all the devices under the control of the DID owner 201, even when the devices have their own public keys. However, in some embodiments it may be useful for each device or some subset of devices under the control of the DID owner 201 to each have their own DID. Thus, in some embodiments the DID creation module 330 may generate an additional DID, for example

DID 331, for each device. The DID creation module 330 would then generate private and public key pairs and DID documents for each of the devices and have them recorded on the distributed ledger 220 in the manner previously described. Such embodiments may be advantageous for devices that may change ownership as it may be possible to associate the device-specific DID to the new owner of the device by granting the new owner authorization rights in the DID document and revoking such rights from the old owner.

[0070] As mentioned, to ensure that the private key 206 is totally in the control of the DID owner 201, the private key 206 is created on the user device 301, browser 302, or operating system 303 that is owned or controlled by the DID owner 201 that executed the DID management module 320. In this way, there is little chance that a third party (and most consequentially, the provider of the DID management module 320) may gain control of the private key 206.

[0071] However, there is a chance that the device storing the private key 206 may be lost by the DID owner 201, which may cause the DID owner 201 to lose access to the DID 205. Accordingly, in some embodiments, the UI 335 may include the option to allow the DID owner 201 to export the private key 206 to an off device secured database 305 that is under the control of the DID owner 201. As an example, the database 305 may be one of the identity hubs 410 described below with respect to Figure 4. A storage module 380 is configured to store data (such as the private key 206 or the attestation information 215 made by or about the DID owner 201) off device in the database 305 or in identity hubs 410 that will be described in more detail to follow. Of course, in some embodiments the storage module 380 may store at least some data on the device if the device has sufficient storage resources. In some embodiments, the private key 206 may be stored as a QR code that may be scanned by the DID owner 201.

[0072] In other embodiments, the DID management module 320 may include a recovery module 360 that may be used to recover a lost private key 206. In operation, the recovery module 360 allows the DID owner 201 to select one or more recovery mechanisms 365 at the time the DID 205 is created that may later be used to recover the lost private key. In those embodiments having the UI 335, the UI 335 may allow the DID owner 201 to provide information that will be used by the one or more recovery mechanisms 365 during recovery. The recovery module 360 may then be run on any device associated with the DID 205.

[0073] The DID management module 320 may also include a revocation module 370 that is used to revoke or sever a device from the DID 205. In operation, the revocation module may use the UI element 335, which may allow the DID owner 201 to indicate a

desire to remove a device from being associated with the DID 205. In one embodiment, the revocation module 370 may access the DID document 210 and may cause that all references to the device be removed from the DID document 210. Alternatively, the public key for the device may be removed. This change in the DID document 210 may then be reflected as an updated transaction on the distributed ledger 220 as previously described.

[0074] Figure 4 illustrates an embodiment of an environment 400 in which a DID such as DID 205 may be utilized. Specifically, the environment 400 will be used to describe the use of the DID 205 in relation to one or more decentralized stores or identity hubs 410 that are each under the control of the DID owner 201 to store data belonging to or regarding the DID owner 201. For instance, data may be stored within the identity hubs using the storage module 380 of Figure 3. It will be noted that Figure 4 may include references to elements first discussed in relation to figures 2 or 3 and thus use the same reference numeral for ease of explanation.

[0075] In one embodiment, the identity hubs 410 may be multiple instances of the same identity hub. This is represented by the line 410A. Thus, the various identity hubs 410 may include at least some of the same data and services. Accordingly, if a change is made to part of at least some of the data (and potentially any part of any of the data) in one of the identity hubs 410, the change may be reflected in one or more of (and perhaps all of) the remaining identity hubs.

[0076] The identity hubs 410 may be any data store that may be in the exclusive control of the DID owner 201. As an example only, the first identity hub 411 and second identity hub 412 are implemented in cloud storage (perhaps within the same cloud, or even on different clouds managed by different cloud providers) and thus may be able to hold a large amount of data. Accordingly, a full set of the data may be stored in these identity hubs.

[0077] However, the identity hubs 413 and 414 may have less memory space. Accordingly, in these identity hubs a descriptor of the data stored in the first and second identity hubs may be included. Alternatively, a record of changes made to the data in other identity hubs may be included. Thus, changes in one of the identity hubs 410 are either fully replicated in the other identity hubs or at least a record or descriptor of that data is recorded in the other identity hubs.

[0078] Because the identity hubs may be multiple instances of the same identity hub, only a full description of the first identity hub 411 will be provided as this description may also apply to the identity hubs 412 through 414. As illustrated, identity hub 411 may include data storage 420. The data storage 420 may be used to store any type of data that is

associated with the DID owner 201. In one embodiment the data may be a collection 422 of a specific type of data corresponding to a specific protocol. For example, the collection 422 may be medical records data that corresponds to a specific protocol for medical data. The collection 422 may include any other type of data, such as attestations 215 made by or about the DID owner 201.

[0079] In one embodiment, the stored data may have different authentication and privacy settings 421 associated with the stored data. For example, a first subset of the data may have a setting 421 that allows the data to be publicly exposed, but that does not include any authentication to the DID owner 201. This type of data may be for relatively unimportant data such as color schemes and the like. A second subset of the data may have a setting 421 that allows the data to be publicly exposed and that includes authentication to the DID owner 201. A third subset of the data may have a setting 421 that encrypts the subset of data with the private key 206 and public key 207 pair (or some other key pair) associated with the DID owner 201. This type of data will require a party to have access to the public key 207 (or to some other associated public key) in order to decrypt the data. This process may also include authentication to the DID owner 201. A fourth subset of the data may have a setting 421 that restricts this data to a subset of third parties. This may require that public keys associated with the subset of third parties be used to decrypt the data. For example, the DID owner 201 may cause the setting 421 to specify that only public keys associated with friends of the DID owner 201 may decrypt this data. With respect to data stored by the storage module 380, these settings 411 may be at least partially composed by the storage module 380 of Figure 3.

[0080] In some embodiments, the identity hub 411 may have a permissions module 430 that allows the DID owner 201 to set specific authorization or permissions for third parties such as third parties 401 and 402 to access the identity hub. For example, the DID owner 201 may provide access permission to his or her spouse to all the data 420. Alternatively, the DID owner 201 may allow access to his or her doctor for any medical records. It will be appreciated that the DID owner 201 may give permission to any number of third parties to access a subset of the data 420. This will be explained in more detail to follow. With respect to data stored by the storage module 380, these access permissions 430 may be at least partially composed by the storage module 380 of Figure 3.

[0081] The identity hub 411 may also have a messaging module 440. In operation, the messaging module allows the identity hub to receive messages such as requests from parties such as third parties 401 and 402 to access the data and services of the identity hub. In

addition, the messaging module 440 allows the identity hub 411 to respond to the messages from the third parties and to also communicate with a DID resolver 450. This will be explained in more detail to follow. The ellipsis 416 represents that the identity hub 411 may have additional services as circumstances warrant.

[0082] In one embodiment, the DID owner 201 may wish to authenticate a new device 301 with the identity hub 411 that is already associated with the DID 205 in the manner previously described. Accordingly, the DID owner 201 may utilize the DID management module 320 associated with the new user device 301 to send a message to the identity hub 411 asserting that the new user device is associated with the DID 205 of the DID owner 201.

[0083] However, the identity hub 411 may not initially recognize the new device as being owned by the DID owner 201. Accordingly, the identity hub 411 may use the messaging module 440 to contact the DID resolver 450. The message sent to the DID resolver 450 may include the DID 205.

[0084] The DID resolver 450 may be a service, application, or module that is configured in operation to search the distributed ledger 220 for DID documents associated with DIDs. Accordingly, in the embodiment the DID resolver 450 may search the distributed ledger 220 using the DID 205, which may result in the DID resolver 450 finding the DID document 210. The DID document 210 may then be provided to the identity hub 411.

[0085] As discussed previously, the DID document 210 may include a public key 208 or 209 that is associated with the new user device 301. To verify that the new user device is owned by the DID owner 201, the identity hub 411 may provide a cryptographic challenge to the new user device 301 using the messaging module 440. This cryptographic challenge will be structured such that only a device having access to the private key 206 will be able to successfully answer the challenge.

[0086] In this embodiment, since the new user device is owned by DID owner 201 and thus has access to the private key 206, the challenge may be successfully answered. The identity hub 411 may then record in the permissions 430 that the new user device 301 is able to access the data and services of the identity hub 411 and also the rest of the identity hubs 410.

[0087] It will be noted that this process of authenticating the new user device 301 was performed without the need for the DID owner 201 to provide any username, password or the like to the provider of the identity hub 411 (i.e., the first cloud storage provider) before the identity hub 411 could be accessed. Rather, the access was determined in a decentralized manner based on the DID 205, the DID document 210, and the associated public and private

keys. Since these were at all times in the control of the DID owner 201, the provider of the identity hub 411 was not involved and thus has no knowledge of the transaction or of any personal information of the DID owner 201.

[0088] In another example embodiment, the DID owner 201 may provide the DID 205 to the third-party entity 401 so that the third party may access data or services stored on the identity hub 411. For example, the DID owner 201 may be a human who is at a scientific conference who desires to allow the third party 401, who is also a human, access to his or her research data. Accordingly, the DID owner 201 may provide the DID 205 to the third party 401.

[0089] Once the third party 401 has access to the DID 205, he or she may access the DID resolver 450 to access the DID document 210. As previously discussed, the DID document 210 may include an end point 213 that is an address or pointer to services associated with the decentralized identity.

[0090] Completing the research data example, the third party 401 may send a message to the messaging module 440 asking for permission to access the research data. The messaging module 440 may then send a message to the DID owner 201 asking if the third party 401 should be given access to the research data. Because the DID owner desires to provide access to this data, the DID owner 201 may allow permission to the third party 401 and this permission may be recorded in the permissions 430.

[0091] The messaging module 440 may then message the third party 401 informing the third party that he or she is able to access the research data. The identity hub 411 and the third party 401 may then directly communicate so that the third party may access the data. It will be noted that in many cases, it will actually be an identity hub associated with the third party 401 that communicates with the identity hub 411. However, it may be a device of the third party 401 that does the communication.

[0092] Advantageously, the above described process allows the identity hub 411 and the third party 401 to communicate and to share the data without the need for the third party to access the identity hub 411 in the conventional manner. Rather, the communication is provisioned in the decentralized manner using the DID 205 and the DID document 210. This advantageously allows the DID owner to be in full control of the process.

[0093] As shown in Figure 4, the third party 402 may also request permission for access to the identity hub 411 using the DID 205 and the DID document 210. Accordingly, the embodiments disclosed herein allow access to any number of third parties to the identity hubs 410.

[0094] As described above, the DID 205 may be used to identify the DID owner 201 when the DID owner interacts with third party entities such as third party entities 401 and 402. Thus, the third parties may be able to view or access the DID 205 since it is being used as the identity. For example, if the interaction with the third party entity is commenting on a blog or the like, then the author of the comment may be identified as "123ABC", which is the DID 205 in the comment section. However, there may be instances where the DID owner 201 may not desire for the DID 205 to be used as an identifier in this manner. Advantageously, the embodiments disclosed herein provide for the selection of pseudonymous names that may be used by the DID owner 201 when he or she interacts with the third party entities.

[0095] Figure 5 illustrates an embodiment of an environment 500 that may be used to generate and select pseudonymous names for use by the DID owner 201. As illustrated, the environment 500 may include a pseudonymous name selection module 510. In one embodiment, the pseudonymous name selection module 510 may be part of or implemented in the DID management module 320 as represented by the dashed line 320A. In other embodiments, the pseudonymous name selection module 510 may be part of or implemented in one of the identity hubs 410 as represented by the dashed line 410A. In still other embodiments, the pseudonymous name selection module 510 may be part of or implemented by a third party such as a provider of the DID management module or the identity hubs. Accordingly, the embodiments disclosed herein are not limited by the location of the pseudonymous name selection module 510.

[0096] The pseudonymous name selection module 510 may include a pseudonymous name generator module 520. In operation, the pseudonymous name generator module 520 may be configured to generate one or more lists of pseudonymous names that may be used by the DID owner 210 for interaction with a third party entity 580, 590, or any number of additional third party entities as illustrated by ellipses 595.

[0097] For example, the pseudonymous name selection module 510 may receive an indication 501 from the DID owner 201 that he or she desires to interact with the third party entities (i.e., third party entities 580 and 590) using a pseudonymous name. In some embodiments, the interaction with the third party entities may be an exchange of DID-related data. The DID-related data may be signed attestation relating to the DID owner 201 or may be an offer to buy or sale goods or services bought and sold by the DID owner 201 and the third party entities. The DID-related data may also be comments or inputs into a written document, a book, a blog, or the like. Thus, the interaction between the DID owner

201 and the third party entities may be any reasonable interaction.

[0098] In response to the indication 501, the pseudonymous name generator module 520 may generate a list 530 of pseudonymous names for use in the interaction. As illustrated, the list 530 may include a first pseudonymous name 531, a second pseudonymous name 532, a third pseudonymous name 533, a fourth pseudonymous name 535, and any number of additional pseudonymous names as illustrated by the ellipses 535. For example, in one embodiments the pseudonymous name 531 may be "Mad Dog", the pseudonymous name 532 may be "Green Frog", the pseudonymous name 533 may be "Mountain Climber", and the pseudonymous name 534 may be "Fast Driver". Thus, it will be noted that the pseudonymous names 531-535 may be any reasonable name that may be used by the DID owner as a substitute identity for the DID 205.

[0099] In some embodiments, the pseudonymous name generator module 520 may generate more than one list of pseudonymous names. For example, the pseudonymous name generator module 520 may generate a list 536 that includes one or more pseudonymous names (not illustrated) and any number of additional lists as illustrated by ellipses 537 that may include one or more pseudonymous names. In such embodiments, the additional lists 536 and 537 may be generated in addition to the list 530 or alternative to the list 530.

[00100] In some embodiments it may be desirable to ensure that the generated pseudonymous names 531-535 are appropriate to a current location of the DID owner 201. For example, suppose the DID owner 201 is a US citizen who is a native English speaker, but who is traveling in France and desires to interact with a French third party entity. In such instance, the use of a pseudonymous name that is based on English or that would only make sense to a native English speaker may not be appropriate to use.

[00101] Accordingly, the pseudonymous name selection module 510 may include a location determination module 540 that is able to determine a current location of the DID owner 201. In some embodiments, the location determination module 540 may be a GPS system or the like that is associated with the user device 301. In operation, the location determination module 540 may determine the current location of the DID owner 201 and then provide this information to the pseudonymous name generator module 520. The pseudonymous name generator module 520 may then use this current location information when generating the list 530 including the pseudonymous names 531-535. For instance, using the example above the pseudonymous name generator module 520 may generate pseudonymous names 531-535 that would be appropriate for use in France and the French language.

[00102] In other embodiments, the location determination module 540 may also be able to determine a current location of a third party entity that the DID owner 201 desires to interact with. For example, suppose the DID owner is a US citizen who is a native English speaker and is currently at his or her home in the US. However, suppose that the third party entity (i.e., third party entities 580 and 590) that the DID owner 201 desires to interact with is located in Japan. In such instance, the use of a pseudonymous name that is based on English or that would only make sense to a native English speaker may not be appropriate to use. Accordingly, the location determination module 540 may determine the current location of the third party entity (i.e., third party entities 580 and 590) and then provide this information to the pseudonymous name generator module 520. The pseudonymous name generator module 520 may then use this current location information when generating the list 530 including the pseudonymous names 531-535. For instance, using the example above the pseudonymous name generator module 520 may generate pseudonymous names 531-535 that would be appropriate for use in Japan and the Japanese language.

[00103] In some embodiments, it may be desirable to ensure that the generated pseudonymous names 531-535 are appropriate for the type of third party entity. For example, suppose that the third party entity 580 is an online gaming community that the DID owner 201 is part of and that the third party entity 590 is a financial institution that the DID owner 201 does business with. As may be appreciated, the types of pseudonymous names 531-535 that may be appropriate for use in the online gaming community may not be appropriate for use with a financial institution.

[00104] Accordingly, in some embodiments the pseudonymous name selection module 510 may include a third party type determination module 560. In operation, the third party type determination module 560 may determine a type 561 of the third party entity 580, a type 562 of the third party entity 590, and any additional types as illustrated by the ellipses 563 of any number of additional third party entities as illustrated by the ellipses 595. In operation, the third party type determination module 560 may provide the types 561, 562, and/or 563 for one or more of the third party entities 580, 590, and 595 to the to the pseudonymous name generator module 520. The pseudonymous name generator module 520 may then use the types 561, 562, and/or 563 when generating the list 530 including the pseudonymous names 531-535.

[00105] For example, the third party type determination module 560 may determine that the third party entity 580 is the online gaming community and may generate the type 561 that specifies “online gaming community” as the type for the third party entity 580. The

third party type determination module 560 may also determine that the third party entity 590 is the financial institution and may generate the type 562 that specifies "financial institution" as the type for the third party entity 590.

[00106] The pseudonymous name generator module 520 may then use the type 561 to determine the pseudonymous names 531-535. In this embodiment such names as the pseudonymous name 531 "Mad Dog", the pseudonymous name 532 "Green Frog", the pseudonymous name 533 "Mountain Climber", and the pseudonymous name 534 "Fast Driver" may all be appropriate for an online gaming community.

[00107] However, these pseudonymous names 531-535 may not be appropriate for the third party entity 590 that is the financial institution. Accordingly, the pseudonymous name generator module 520 may use type 562 to determine the pseudonymous names 531-535 that are more appropriate for interaction with a financial institution. For example, such names as a pseudonymous name 531 "Banker 100", a pseudonymous name 532 "Banker 200", a pseudonymous name 533 "Investor 100", and a pseudonymous name 534 "Investor 200" may all be appropriate for a financial institution.

[00108] In some embodiments, the pseudonymous name generator module 520 may generate the list 530 for interaction with the third party entity 580 that is the online gaming community and the list 536 for interaction with the third party entity 590 that is the financial institution simultaneously or at near the same time. In this way, the DID owner 201 may have more than one list of pseudonymous names at a time that may be selected for use in interaction with more than one third party entity simultaneously or at near the same time.

[00109] Once the list 530 including the pseudonymous names 531-535 (or the other lists 536 or 537) is generated, the pseudonymous name selection module 510 may receive a selection that selects a specific one of the pseudonymous names for use in the interaction with the third party entity. In one embodiment, the list 530 including the pseudonymous names 531-535 (or the other lists 536 or 537) may be displayed to the DID owner 201. The DID owner 201 may then provide a selection 502 that selects the specific pseudonymous name for use in the interaction with the third party entity. For example, in the example embodiment where the third party entity 580 is an online gaming community, the DID owner 201 may input the selection 502 to select the pseudonymous name 532 "Green Frog" for use in interacting with the online gaming community.

[00110] In some embodiments, the selection may be automatically generated by the pseudonymous name selection module 510. Accordingly, the pseudonymous name selection module 510 may include an automatic selection module 570 that provides a

selection 571 that selects the specific pseudonymous name for use in the interaction. In one embodiment, the automatic selection 571 may be based on one or more user selected rules 551, 552, or any number of additional rules as illustrated by ellipses 533 that are input into a rules module 550 by the DID owner 201. The rules 551-553 may specify criteria that should be used when selecting the pseudonymous name. For instance, a rule 531 may specify that a specific pseudonymous name always be used for a particular type of third party entity. A rule 532 may specify that a different pseudonymous name should be used for every visit to the same third party entity. A rule 553 may specify that a pseudonymous name should never be used more than once in all interactions with all third parties.

[00111] In other embodiments, the automatic selection 571 may be based on the type of the third party entity. In such embodiments, the automatic selection module 570 may be configured to select one of the pseudonymous names generated using the third party type module as previously described that is best for the particular situation.

[00112] Once the specific pseudonymous name has been selected, a binding module 575 of the pseudonymous name selection module 510 may generate a binding 576 that binds the DID 205 to the selected pseudonymous name. The binding 576 ensures that the selected pseudonymous name may be used by the DID owner 201 in place of the DID 205 during interactions with the third party entities.

[00113] For example, as shown in Figure 5 the DID owner 201 may interact with the third party entity 580 by exchanging some form of DID related data 581. As shown, the DID-related data 581 includes an example of the binding 576 that has bound the DID 205 to the pseudonymous name 531. For instance, the DID-related data may be a blog post generated by the third party entity 580 and the DID owner 201 may desire to post a comment in the blog. Accordingly, the binding 576 that binds the DID 205 to the pseudonymous name 531 allows the pseudonymous name 531 to be used as the author of the comment without the need to show or display the DID 205.

[00114] Likewise, as shown in Figure 5 the DID owner 201 may interact with the third party entity 590 by exchanging some form of DID related data 591. As shown, the DID-related data 591 includes an example of the binding 576 that has bound the DID 205 to the pseudonymous name 532. For example, the DID-related data may be a product for sale by the third party entity 590 and the DID owner 201 may desire to make an offer to buy the product. Accordingly, the binding 576 that binds the DID 205 to the pseudonymous name 532 allows the pseudonymous name 532 to be used in the offer to buy the product without the need to show or display the DID 205.

[00115] The following discussion now refers to a number of methods and method acts that may be performed. Although the method acts may be discussed in a certain order or illustrated in a flow chart as occurring in a particular order, no particular ordering is required unless specifically stated, or required because an act is dependent on another act being completed prior to the act being performed.

[00116] Figure 6 illustrates a flow chart of an example method 600 for a method for generating one or more pseudonymous names for use by a DID owner when interacting with third party entities. The method 600 will be described with respect to one or more of Figures 1-5 discussed previously.

[00117] The method 600 includes receiving an indication from a DID owner who is associated with a DID that the DID owner desires to interact with one or more third party entities (610). For example, as previously described the pseudonymous name selection module 510 may receive the indication 501 from the DID owner 201 who is associated with the DID 205 that he or she desires to interact with the third party entities 580, 590, and/or 595.

[00118] The method 600 includes generating a list of one or more pseudonymous names that are to be used in place of the DID as the DID owner interacts with the one or more third party entities (620). For example, as previously described the pseudonymous name selection module 510 may generate the list 530 that includes the pseudonymous names 531-535. The lists 536 and 537 may also be generated.

[00119] The method 600 includes receiving a selection for a specific one of the generated one or more pseudonymous names (630). For example, as previously described the pseudonymous name selection module 510 may receive the selection 502 from the DID owner 201 or the automatic selection 571 that selects a specific pseudonymous name.

[00120] The method 600 includes binding the selected specific pseudonymous name to the DID so that the selected specific pseudonymous name is used during the interaction (640). For example, as previously described the pseudonymous name selection module 510 may generate the binding 576 that binds the DID 205 to the selected pseudonymous name. This ensures that the selected pseudonymous name is used during the interaction with the third party entities.

[00121] For the processes and methods disclosed herein, the operations performed in the processes and methods may be implemented in differing order. Furthermore, the outlined operations are only provided as examples, and some of the operations may be optional, combined into fewer steps and operations, supplemented with further operations, or

expanded into additional operations without detracting from the essence of the disclosed embodiments.

[00122] The present invention may be embodied in other specific forms without departing from its spirit or characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. The scope of the invention is, therefore, indicated by the appended claims rather than by the foregoing description. All changes which come within the meaning and range of equivalency of the claims are to be embraced within their scope.

CLAIMS

1. A computing system that is implemented in a decentralized network that implements a distributed ledger, the distributed ledger being configured to back one or more decentralized identities (DID) for one or more users of the computing system, the computing system comprising:

one or more processors; and

one or more computer-readable media having thereon computer-executable instructions that are structured such that, when executed by the one or more processors, cause the computing system to:

receive an indication from a DID owner who is associated with a DID that the DID owner desires to interact with one or more third party entities;

generate a list of one or more pseudonymous names that are to be used in place of the DID as the DID owner interacts with the one or more third party entities;

receive a selection for a specific one of the generated one or more pseudonymous names; and

bind the selected specific pseudonymous name to the DID so that the selected specific pseudonymous name is used during the interaction.

2. The computing system of claim 1, wherein the interaction with the one or more third party entities is an exchange of DID-related data.

3. The computing system of claim 1, wherein the computer executable instructions are further structured to cause the computing system to:

determine a current location of the DID owner; and

include in the generated list one or more pseudonymous names that are appropriate for the current location of the DID owner.

4. The computing system of claim 1, wherein the computer executable instructions are further structured to cause the computing system to:

determine a current location of the one or more third party entities; and

include in the generated list one or more pseudonymous names that are appropriate for the current location of the one or more third party entities.

5. The computing system of claim 1, wherein the selection is received from the DID owner.

6. The computing system of claim 1, wherein the selection is generated automatically by the computing system.

7. The computing system of claim 6, wherein the automatic selection is based

on one or more rules that are input by the DID owner or is based on a type of the one or more third party entities.

8. The computing system of claim 1, wherein the computer executable instructions are further structured to cause the computing system to:

determine a type of the one or more third party entities; and

include in the generated list one or more pseudonymous names that are appropriate for the type of the one or more third party entities.

9. In a computing system that is implemented in a decentralized network that implements a distributed ledger, the distributed ledger being configured to back one or more decentralized identities (DID) for one or more users of the computing system, a method for generating one or more pseudonymous names for use by a DID owner when interacting with third party entities, the method comprising:

receiving an indication from a DID owner who is associated with a DID that the DID owner desires to interact with one or more third party entities;

generating a list of one or more pseudonymous names that are to be used in place of the DID as the DID owner interacts with the one or more third party entities;

receiving a selection for a specific one of the generated one or more pseudonymous names; and

binding the selected specific pseudonymous name to the DID so that the selected specific pseudonymous name is used during the interaction.

10. A computer program product comprising one or more computer-readable storage media having thereon computer-executable instructions that are structured such that, when executed by one or more processors of a computing system, cause the computing system to perform a method for generating one or more pseudonymous names for use by a DID owner when interacting with third party entities, the method comprising:

receiving an indication from a DID owner who is associated with a DID that the DID owner desires to interact with one or more third party entities;

generating a list of one or more pseudonymous names that are to be used in place of the DID as the DID owner interacts with the one or more third party entities;

receiving a selection for a specific one of the generated one or more pseudonymous names; and

binding the selected specific pseudonymous name to the DID so that the selected specific pseudonymous name is used during the interaction.

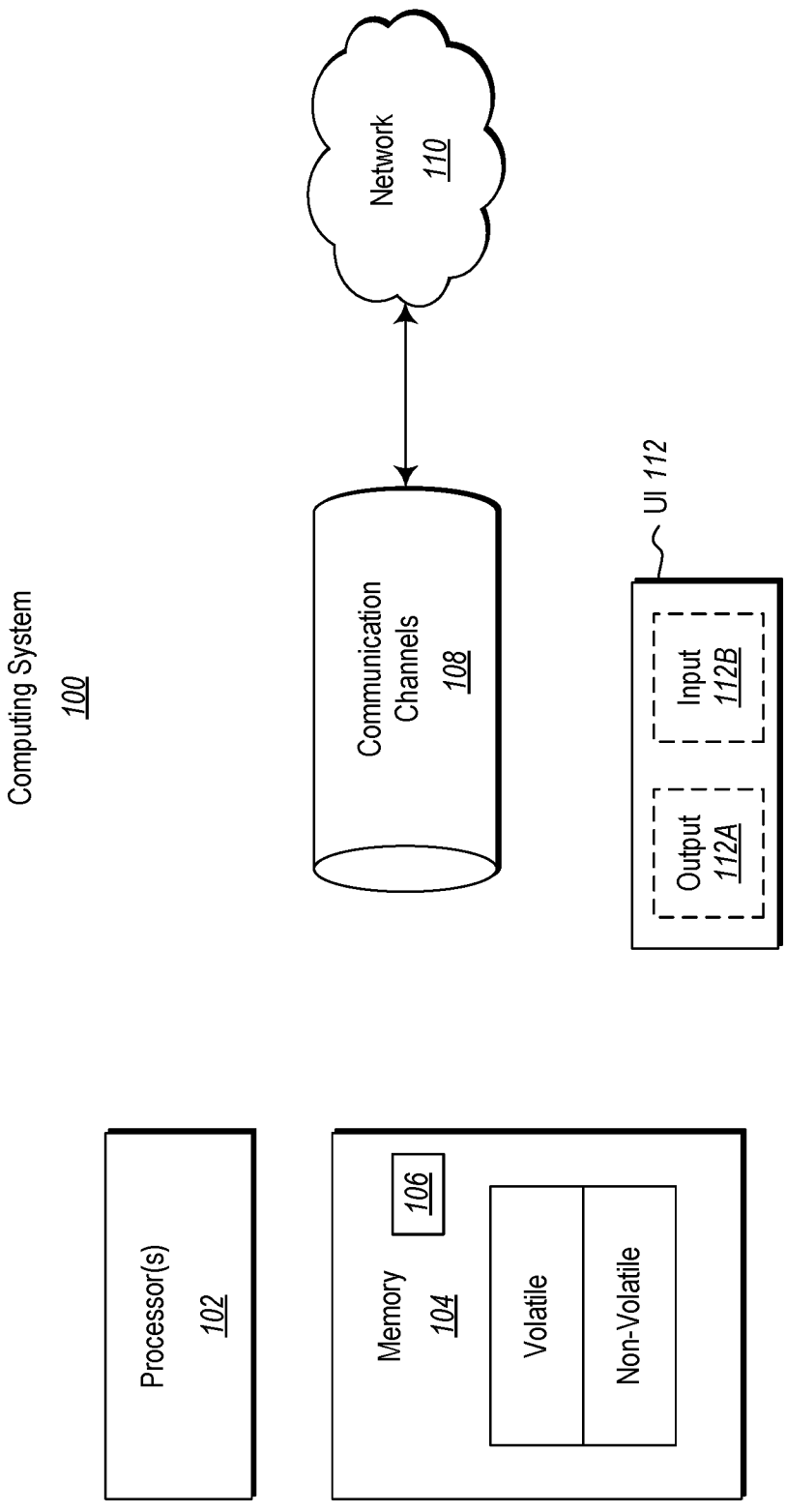

Computing System
100
Network
110
Communication Channels
108
UI 112
Output
112A
Input
112B
Processor(s)
102
Memory
104
106
Volatile
Non-Volatile

FIG. 1

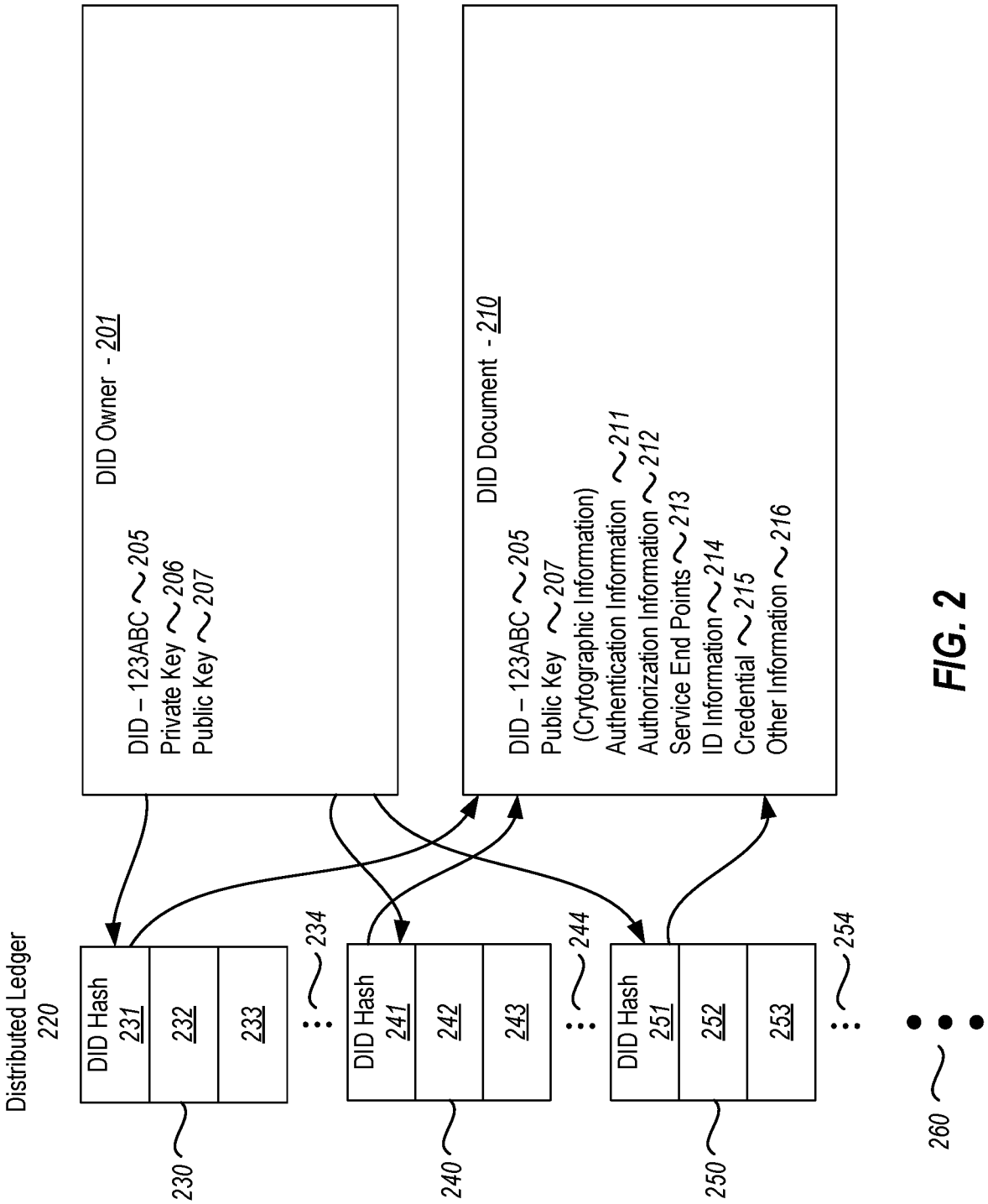

DID Owner - 201
DID – 123ABC ~ 205
Private Key ~ 206
Public Key ~ 207
DID Document - 210
DID – 123ABC ~ 205
Public Key ~ 207
(Crytographic Information)
Authentication Information ~ 211
Authorization Information ~ 212
Service End Points ~ 213
ID Information ~ 214
Credential ~ 215
Other Information ~ 216
Distributed Ledger
220
DID Hash
231
232
233
234
DID Hash
241
242
243
244
DID Hash
251
252
253
254
230
240
250
260

FIG. 2

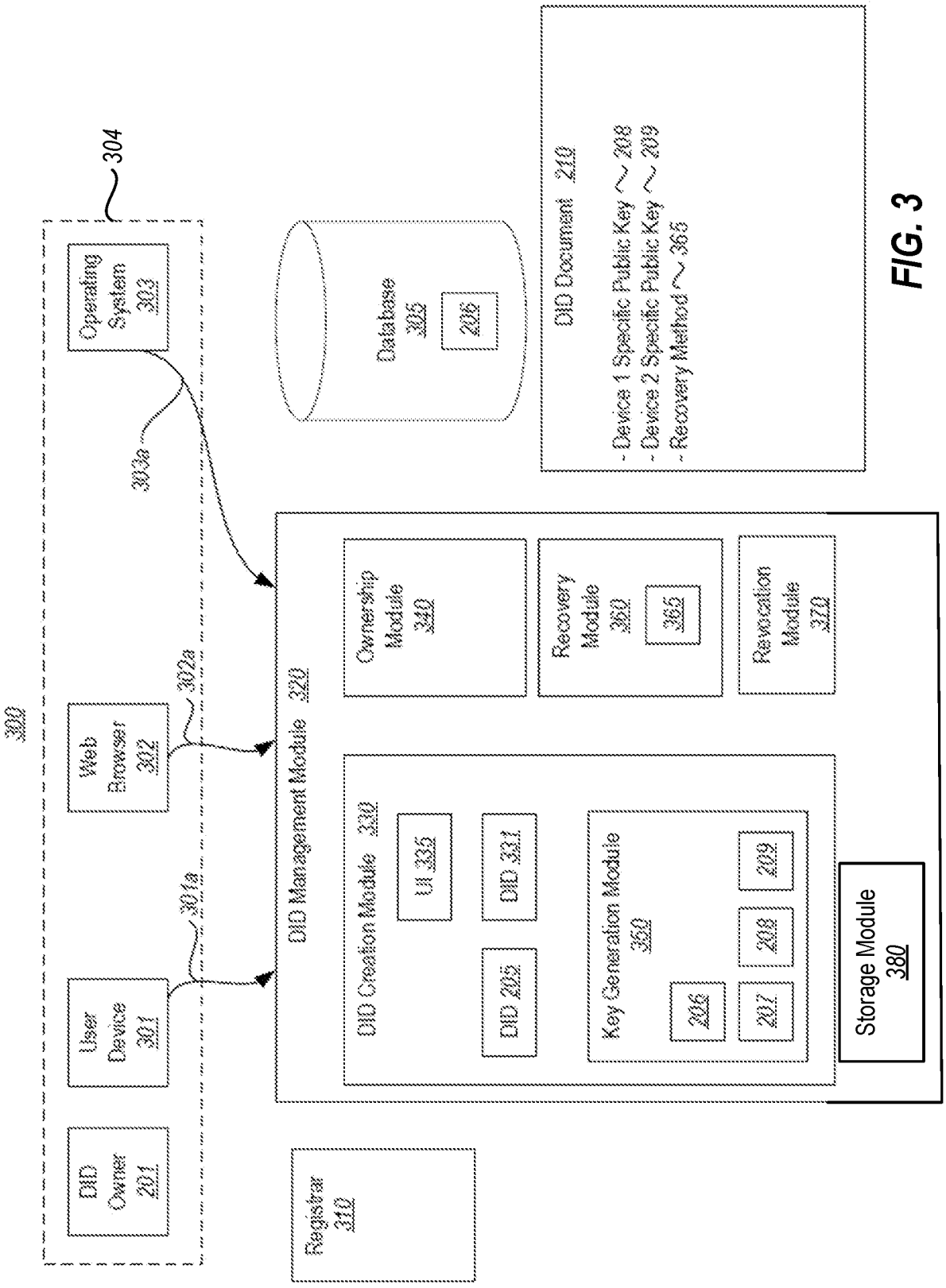

300
304
Operating System 303
303a
Web Browser 302
302a
User Device 301
301a
DID Owner 201
Registrar 310
Database 305
206
DID Document 210
- Device 1 Specific Public Key ~ 208
- Device 2 Specific Public Key ~ 209
- Recovery Method ~ 365
DID Management Module 320
Ownership Module 340
Recovery Module 360
365
Revocation Module 370
DID Creation Module 330
UI 335
DID 331
DID 205
Key Generation Module 350
206
207
208
209
Storage Module 380

FIG. 3

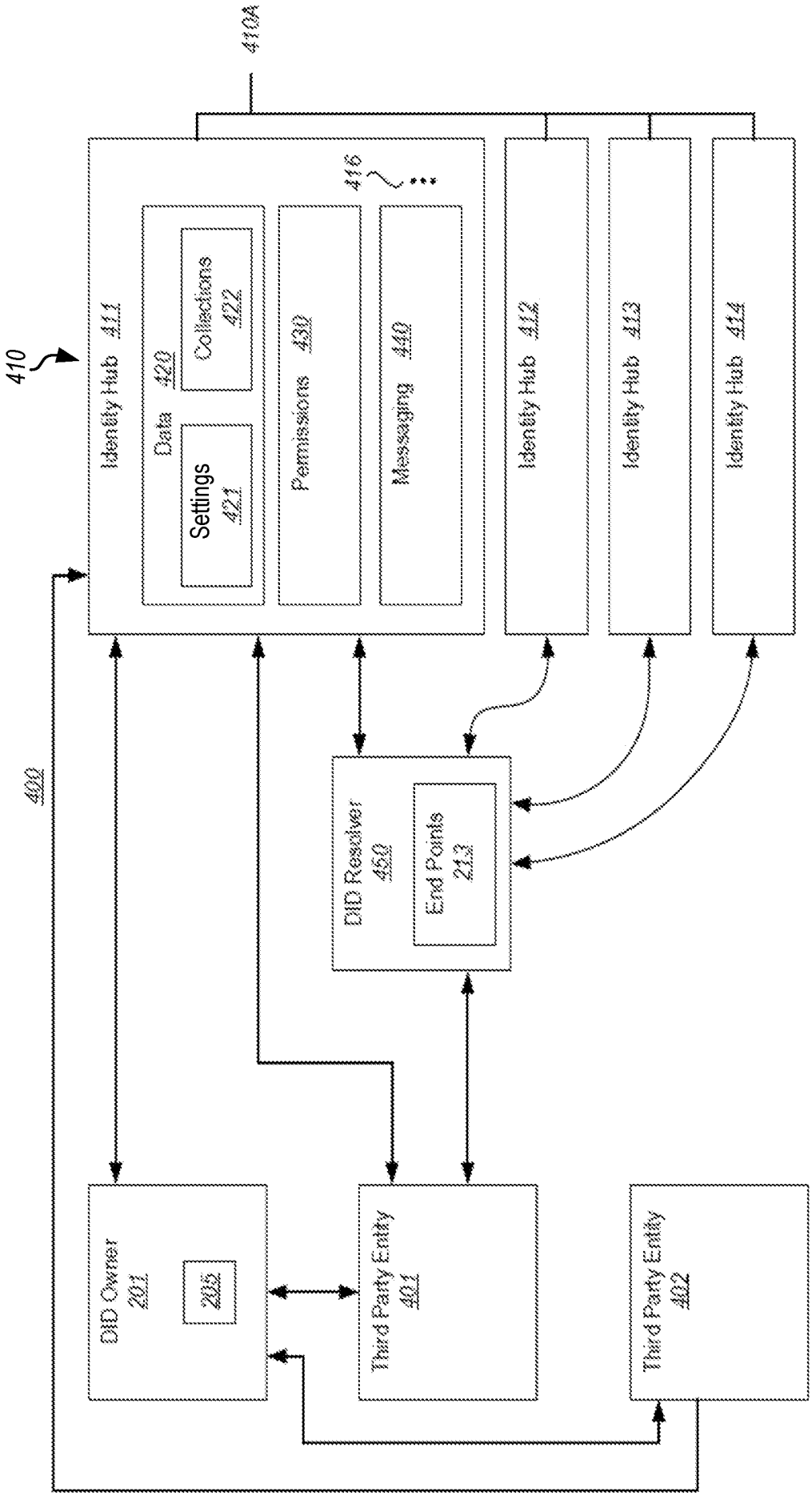

410A
410
Identity Hub 411
Data 420
Collections 422
Settings 421
Permissions 430
Messaging 440
416
Identity Hub 412
Identity Hub 413
Identity Hub 414
400
DID Resolver 450
End Points 213
DID Owner 201
205
Third Party Entity 401
Third Party Entity 402

FIG. 4

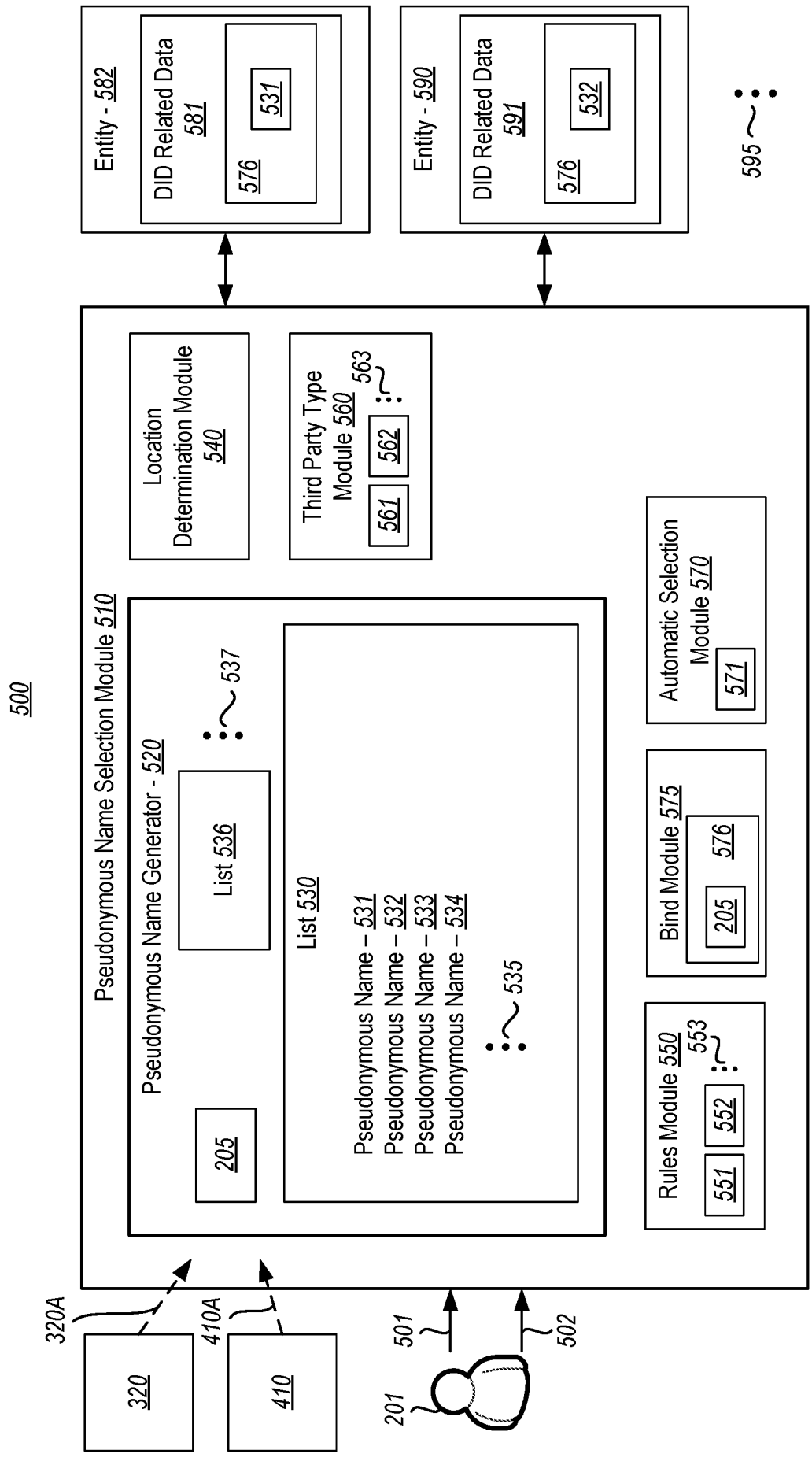

500
Pseudonymous Name Selection Module 510
Pseudonymous Name Generator - 520
205
List 536
537
List 530
Pseudonymous Name – 531
Pseudonymous Name – 532
Pseudonymous Name – 533
Pseudonymous Name – 534
535
Location Determination Module 540
Third Party Type Module 560
561
562
563
Rules Module 550
551
552
553
Bind Module 575
205
576
Automatic Selection Module 570
571
Entity - 582
DID Related Data 581
576
531
Entity - 590
DID Related Data 591
576
532
595
320A
320
410A
410
501
502
201

FIG. 5

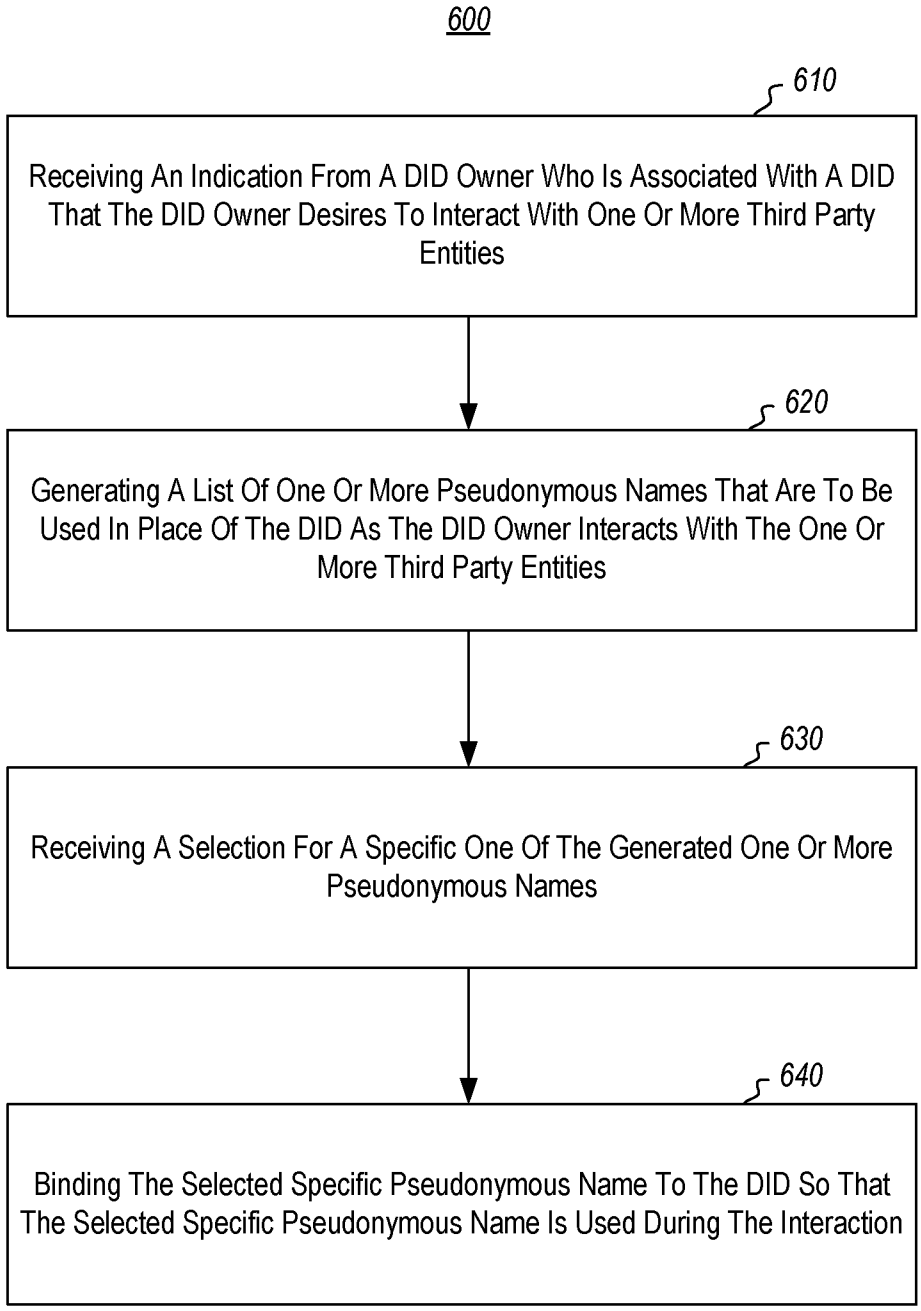

600
610
Receiving An Indication From A DID Owner Who Is Associated With A DID That The DID Owner Desires To Interact With One Or More Third Party Entities
620
Generating A List Of One Or More Pseudonymous Names That Are To Be Used In Place Of The DID As The DID Owner Interacts With The One Or More Third Party Entities
630
Receiving A Selection For A Specific One Of The Generated One Or More Pseudonymous Names
640
Binding The Selected Specific Pseudonymous Name To The DID So That The Selected Specific Pseudonymous Name Is Used During The Interaction

FIG. 6

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2020/026030

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/32 G06F21/62 H04L29/06
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

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	CN 109 561 383 A (UNIV KUNMING SCIENCE & TECH) 2 April 2019 (2019-04-02) par. 1-8	1-10
A	US 2018/307859 A1 (LAFEVER MALCOLM GARY [US] ET AL) 25 October 2018 (2018-10-25) par. 36, 54, 55, 138, 185, 191, 242, 454, 574, 636, 701, 709-720	1-10
A	CN 108 492 550 A (JINAN INSPUR HI TECH INVEST & DEVELOPMENT CO LTD) 4 September 2018 (2018-09-04) par. 1, 14, 17, 21, 22, 24-27	1-10
A	CN 105 681 320 A (UNIV CHONGQING POSTS & TELECOM) 15 June 2016 (2016-06-15) abstract	1-10

-/--

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

[X] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
6 July 2020	16/07/2020

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	Murgan, Tudor A.

1

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2020/026030

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 107 396 285 A (SHENZHEN INST OF ADV TECH CAS) 24 November 2017 (2017-11-24) step S201 of Fig. 2; par. 11, 12	1-10
A	US 2014/359782 A1 (GOLIC JOVAN [IT]) 4 December 2014 (2014-12-04) abstract	1-10

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2020/026030

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
CN 109561383 A	02-04-2019	NONE	
US 2018307859 A1	25-10-2018	NONE	
CN 108492550 A	04-09-2018	NONE	
CN 105681320 A	15-06-2016	NONE	
CN 107396285 A	24-11-2017	NONE	
US 2014359782 A1	04-12-2014	AR 089484 A1	27-08-2014
		BR 112014015694 A2	13-06-2017
		CN 104094573 A	08-10-2014
		EP 2798809 A1	05-11-2014
		ES 2565842 T3	07-04-2016
		IL 233314 A	30-03-2017
		US 2014359782 A1	04-12-2014
		WO 2013097886 A1	04-07-2013