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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 July 2023 (13.07.2023)

WIPO | PCT

(10) International Publication Number
WO 2023/133521 A1

(51) International Patent Classification:
G06F 21/33 (2013.01) *H04M 7/00* (2006.01)
G06Q 20/38 (2012.01) *H04L 9/00* (2022.01)
G06Q 20/40 (2012.01) *H04L 9/32* (2006.01)
G06Q 20/02 (2012.01) *H04L 9/40* (2022.01)

(21) International Application Number:
PCT/US2023/060252

(22) International Filing Date:
06 January 2023 (06.01.2023)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
63/266,560 07 January 2022 (07.01.2022) US

(71) Applicant: **GCOM SOFTWARE LLC** [US/US]; 9175 Guilford Road, Suite 101, Columbia, Maryland 21046 (US).

(72) Inventors: **PURI, Rahul**; 9175 Guilford Road, Suite 101, Columbia, Maryland 21046 (US). **FERREIRA, Andrew**; 9175 Guilford Road, Suite 101, Columbia, Maryland 21046 (US). **JACKSON, Ivan**; 9175 Guilford Road, Suite 101, Columbia, Maryland 21046 (US). **BHATNAGAR, Piyush**; 9175 Guilford Road, Suite 101, Columbia, Maryland 21046 (US).

(74) Agent: **SINGER, James** et al.; 997 Lenox Drive, Building 3, Lawrenceville, New Jersey 08648-2311 (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS,

(54) Title: METHOD AND SYSTEM FOR DIGITAL IDENTITY AND TRANSACTION VERIFICATION

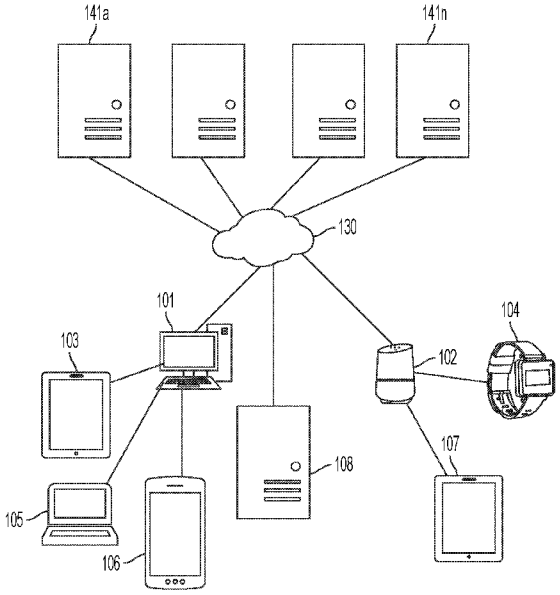

FIG. 1

(57) Abstract: Methods of determining whether to trust an entity before sharing information with the entity, as well as methods of verifying whether to trust information received from an entity, are disclosed. In the processes, two entities, referred to as a holder and a verifier, desire to engage in an exchange of digital information. Before the holder will share information with the verifier, the holder will determine whether the verifier is a trusted entity. Before the verifier trusts information that it receives from the holder, it will examine a proof that it received from the holder to determine whether the proof includes information from or about a trusted third party referred to as an issuer. Information from an identity authority may be used in each of these verification steps.

WO 2023/133521 A1

[Continued on next page]

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, CV, 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, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

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

TITLE: METHOD AND SYSTEM FOR DIGITAL IDENTITY AND TRANSACTION VERIFICATION

RELATED APPLICATIONS AND CLAIM OF PRIORITY

[0001] This patent document claims priority to United States provisional patent application number 63/266,560, filed January 7, 2022. The disclosure of the priority application is fully incorporated into this document by reference.

BACKGROUND

[0002] Systems that verify the identity of a participant in a transaction, data provided a participant, or both are critical for modern electronic transactions. For example, when an individual makes an application to a government agency or transacts with a business, it is critical for the agency or business to be able to verify the identity of the individual. This ensures both security of the entity's systems and integrity of the entity's data. In addition, when the individual receives a request for information from the agency or business, it is important that the individual be able to verify the identity of the requesting party to ensure that the request is not a phish, scan or spoof that in which a bad actor is attempting to get compromising information from the individual. Also critical to digital transactions is the ability for an individual or organization to know whether to trust data received from another entity.

[0003] Current systems for identity and data verification can be cumbersome and time-consuming. Individuals may be required to fill out long forms with personal data, sometimes repeatedly, which can be a tedious process that potentially exposes the entity to fraud and the individual to identity theft. The existing processes are also error-prone and can result in the collection of inconsistent or inaccurate data, which can lead to processing delays, inappropriate

denials of service, or both. In addition, entities such as agencies and businesses may need to spend significant time and resources to verify individual digital identities, and acquire, verify, store and manage large volumes of data.

[0004] This document describes methods and systems that are directed to the problems described above, and/or other issues.

SUMMARY

[0005] In various embodiments, users of mobile electronic devices that run a verification application will communicate with other electronic devices that are part of a blockchain infrastructure. Each mobile device includes or accesses a secure data storage medium housing verification information for entities that may participate in transactions with other entities such as government agencies or businesses. When a user of such a device initiates a transaction, verified information is transferred between organizations or individuals. The transaction itself may or may not be saved to the blockchain. An entity using another device with the verification app may then wish to authoritatively prove they are interacting with a trusted organization.

[0006] In some embodiments, a method of verifying whether to share information with an entity comprises, by an electronic device of a holder (i) receiving a data request from an electronic device of a verifier; (ii) determining whether the verifier is a trusted entity by: (a) if the data request includes an identity authority (IA) token, using the IA token to determine whether the verifier is a trusted entity, and (b) if the data request does not include the IA token, using a decentralized identifier (DID) for the verifier that was included in the data request to determine whether the verifier is a trusted entity; and (iii) upon determining that the verifier is a trusted entity, providing data to the verifier in response to the data request, otherwise rejecting the data request.

[0007] In some embodiments, a method of verifying whether to trust information received from an entity comprises, by an electronic device of a verifier: (i) sending a data request to an electronic device of a holder; (ii) in response to the data request, receiving data and a proof from the holder, wherein the proof comprises a DID

[0008] and a signature of an issuer; (iii) determining whether the data is associated with a trusted issuer by: (a) examining the proof to determine whether the proof also includes an identity authority (IA) token, (b) if the proof includes an IA token that was issued by a known IA, using the IA token to determine whether the issuer is a trusted entity, and (c) if the proof does not include the IA token, using the DID for the issuer that is in the proof to determine whether the issuer is a trusted entity; and (iv) upon determining that the issuer is a trusted entity, accepting the proof and using the data, otherwise rejecting the proof and the data.

[0009] In some embodiments, before the verifier sends the data request to the electronic device of the holder, the issuer may present the DID for the issuer to the known IA in a request for the IA token from the known IA, receive the IA token from the known IA in response to the request for the IA token, and write the DID for the issuer to a distributed ledger.

[0010] Some embodiments may combine any or all of the methods described above.

[0011] The methods described above may be embodied in a system including a processor and memory containing programming instructions that, when executed, will cause the processor to implement the actions described above. Various embodiments also include a computer program product that contains such programming instructions, and a memory containing the computer program product.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] FIG. 1 illustrates an example system infrastructure in accordance with various embodiments.

[0013] FIG. 2 illustrates an example process flow for identity and data verification in graphic format.

[0014] FIGs. 3A and 3B illustrate the process flow of FIG. 2 in a flowchart format.

[0015] FIG. 4 provides additional detail about certain steps of the process of FIGs. 2 and 3A-3B.

[0016] FIG. 5 provides additional detail about certain other steps of the process of FIGs. 2 and 3A-3B.

[0017] FIG. 6 provides additional detail about certain other steps of the process of FIGs. 2 and 3A-3B.

[0018] FIG. 7 illustrates an example user interface for an identity and data verification application for a user electronic device.

[0019] FIG. 8 illustrates an example blockchain data structure.

[0020] FIG. 9 is a block diagram that illustrates example components of an electronic device that may be used in connection with the system.

DETAILED DESCRIPTION

[0021] As used in this document, the singular forms “a,” “an,” and “the” include plural references unless the context clearly dictates otherwise. Unless defined otherwise, all technical and scientific terms used herein have the same meanings as commonly understood by one of ordinary skill in the art. As used in this document, the term “comprising” (or “comprises”) means

"including (or includes), but not limited to." When used in this document, the term "exemplary" is intended to mean "by way of example" and is not intended to indicate that a particular exemplary item is preferred or required.

[0022] In this document, when terms such "first" and "second" are used to modify a noun, such use is simply intended to distinguish one item from another, and is not intended to require a sequential order unless specifically stated. The term "approximately," when used in connection with a numeric value, is intended to include values that are close to, but not exactly, the number. For example, in some embodiments, the term "approximately" may include values that are within +/- 10 percent of the value.

[0023] Additional terms that are relevant to this disclosure will be defined at the end of this Detailed Description section.

[0024] This document describes a decentralized method and system for authoritatively verifying the digital identity of one or more participants in an online transaction, and also for verifying data provided in the transaction. Furthermore, a method is provided wherein the identities of the verifier(s) and issuer(s) may be verified via a trusted entity. Digital verification systems that use distributed ledgers (i.e., blockchain infrastructure) are currently known. However, when using a public ledger, the information that is placed on the ledger in current methods and systems is by definition accessible to the public. This creates a problem when an entity needs to verify an individual's personal information such as name, address, date of birth, government-issued credential (such as Social Security Number or driver's license number), vaccination records, employment records and the like, as the individual will not want this information to be public and instead want to control who has access to this information.

[0025] The decentralized verification solution described in this document verifies a user's personal information once and allows each user to store that information in a secure data storage medium on their electronic devices or on a cloud-based server. Users can share data when needed, but the users' identities and data can be independently verifiable using information that is stored on the blockchain.

[0026] In the processes below, each participant in the process will be associated with a unique decentralized identifier (DID). DIDs, as are known in the art, are a type of uniform resource identifier (URI) that uniquely refer to an entity as determined by that entity, rather than be a centralized registry, identity provider, or certificate authority. A DID may include a DID document, which is a set of data describing the entity that is the DID subject, along with a mechanism such as a cryptographic public key that the entity or its delegate can use to authenticate itself and prove its association with the DID.

[0027] FIG. 1 illustrates an example system in which multiple electronic devices **101-108** communicate with each other and/or one or more external electronic devices**.** The communication may be via a near-field communication protocol such as Bluetooth or Bluetooth Low Energy, via a short-range communication protocol, via one or more communication network **130** such as via wi-fi or another local area network, a wide area network, a mobile communication network, or by other communication protocols.

[0028] The electronic devices **101-108** may be in communication with any number of blockchain infrastructure electronic devices **141a…141n** via one or more communication networks **130**. The blockchain infrastructure electronic devices **141a…141n** may each have data stores that, along with other electronic devices, collectively hold data elements of a distributed ledger (i.e., a blockchain).

[0029] Any or all of the electronic devices **101-108** may be configured with programming to run a digital verification application. Each device that runs the verification application may operate as an electronic device of a holder, an issuer, a verifier, or an identity authority, as each will be described in more detail below. Example applications, and processes that such applications (along with server applications) may implement, include without limitation issuing and verification of state driver's license information, government benefits applications, and other government-issued licenses.

[0030] FIGs. 2, 3A and 3B illustrate an example process flow by which an electronic device of an entity referred to as a "verifier" **203** may verify the identity of, and choose whether or not to trust information provided by, a "holder" **201**, and by which the holder **201** may confirm the identity of the verifier **203** and choose whether or not to share data with the verifier **203**. In addition to verifying the content of the information and that the holder **201** has not altered the data since receiving it, the verifier **203** may need to verify that the issuer **202** (which typically, but not necessarily, may be a governmental agency, business, or other organization) is legitimate. This document uses the terms "verifier," "issuer" and "holder" to reflect the fact that the holder is a user (such as an individual) of a secure data storage application that holds personal information associated with the issuer **202**, while the issuer **202** is an entity that delivers a verifiable credential to the holder **201**. After the holder **201** receives the issuer's credential, the verifier **203** may use the credential to verify that data received from the holder **201** is trusted data.

[0031] The verifier **203** can verify the identity of the issuer **202** with the assistance of a verifying entity (referred to as an "identity authority" **205**), which may be itself be an issuer, or it may be a system that is external to all the other participants shown in FIG. 2. The verifier **203**

performs certain of the verification functions that are described in this document using information stored on an application in a distributed digital ledger **204**.

[0032] With reference to FIGs. 2-6, before the verification described above begins, at step **301** an identity authority **205** will write one or more verifiable identifying entries for the identity authority to the distributed ledger **204**. The identity authority **205** is a publicly known entity that publishes their public DID online. As used in this document an "identifying entry" is a one-time, initial entry that an entity writes to a digital ledger to identify itself. As shown in FIG. 4, the identifying entries **405** for the identity authority will include a DID for the identity authority, along with a schema and a credential definition for the identity authority's DID. The identity authority credential also will include a verification key, which is a public key that can be used to verify the authenticity of one or more identify authority tokens ("IA tokens"), which have a a use that will be described below.

[0033] At step **302** the issuer **202** also will write one or more of its identifying entries to the distributed ledger **204**. As shown in FIG. 4, the issuer's identifying entries **402** will include a DID for the issuer, along with a schema and a credential definition for the issuer's DID.

[0034] At step **303** the issuer will contact the identity authority to request an IA token. In connection with this request, the issuer will present the issuer's DID, optionally with other attributes such as, for example, a web uniform reference locator (URL), a legal name, and/or other identifying information to the identity authority.

[0035] At **304** the identity authority will attempt to verify the issuer. The identity authority may do this by, for example, requiring the issuer to prove that it owns the private key associated with the DID and/or to prove that it has control of or a legal right to use the identifying information provided. This may happen in several possible ways, such as by

examining the issuer's DID and determining whether it matches the public issuer DID that the issuer wrote to the distributed ledger, or by providing the information to a human analyzer to review and return a response. If the identity authority does not verify the issuer at **304**, then the process ends. However, if verification of the issuer occurs at step **304,** at step **305** the identity authority **205** will then give an IA token to the issuer **202**, write the IA token to the ledger **204**, or both. As shown in FIG. 5, in which the identity authority shares the IA token **505** with the issuer **202**, the IA token **505** will include the public DID for the identity authority and the issuer's DID, and it will be signed using a signature created with the identity authority's private key. The IA token **505** also may include other data describing or relating to the identity authority, issuer, or other entities or processes. The issuer may then use the IA token or information from it in an issuer credential, which (as described below) a verifier can use to verify authenticity of an issuer or holder later in the process.

[0036] At step **306** the issuer will present a verifiable credential to the holder. FIG. 2 indicates that the presentation of a verifiable credential may include presentation (step **306b**) of the credential in response to receipt of a request for the verifiable credential from the holder (step **306a**). This may happen, for example, by the holder logging into a website or other service that the issuer provides or is affiliated with, and filling out a form or otherwise providing certain data (such as a social security number, driver's license number, or other personal information, or by scanning a QR code or other barcode) in order to prove that the holder is entitled to receive the data. Alternatively, the issuer may present the verifiable credential to the holder on its own initiative, such as in response to an update to the credential or an offline request to provide the credential to the holder.

[0037] As shown in FIG. 6, the verifiable credential **602** of the issuer will include the issuer DID and a signature created with the issuer's private key. If the identity authority provided the issuer with an IA token, the verifiable credential **602** also will include that IA token (which includes at least the issuing authority's public DID, the issuer's public DID, and a signature created by the issuing authority). The verifiable credential **602** also may include, or may be provided along with, data that will be required to respond to a data request from a verifier. As will be described below, a verifier can (i) use the combination of the issuer's DID and public key to verify that the credential did in fact come from that issuer and was issued to the holder, and (ii) use the IA token (whether acquired directly from the holder or subsequently using some other query) verify that an issuer with which the verifier may not have a previous trust relationship can be permitted to provide verified data

[0038] At some point, in response to a need to initiate a transaction between the holder and a verifier **203**, the verifier **203** requests data from the holder **201**. For example, as noted above if the holder requests a service from the verifier, the verifier may require the holder to provide social security information, driver's license information, or other data that the holder received from the issuer, or that the holder derived from such issued data. To do that, the verifier will send a request for the data to the holder, along with (or as part of) a proof request. However, before doing that, at **307** the verifier examines its internal data store to decide whether it has its own IA token to present to the holder. If it does **(307: YES)**, then the process proceeds to step **321** described below. Otherwise (**307: NO**), the process proceeds to step **311** described below.

[0039] If the verifier **203** does not have its own IA token (**307: NO**), then at **311** the verifier **203** sends the proof request to the holder **201** and passes its own public DID to the holder **201** with the request. At **312**, upon receiving the request from the verifier at **311**, the holder **201,**

upon identifying that the request does not include an IA token, uses the verifier's DID to look up the verifier's IA token, either on the ledger or by direct request to an IA that the holder trusts. The holder then uses information from the IA token to determine whether to trust the verifier. Alternatively, the holder may send the verifier's DID to a trusted IA with a request to respond with information that the holder may use to determine whether to trust the verifier. Such information may include, for example, a human-readable name or a website URL.

[0040] If the verifier **203** has its own IA token (**307: YES**), then at **321** the verifier **203** sends the request to the holder **201** along with the verifier's IA token (which contains the verifier's public DID). At step **322**, upon receiving the request from step **321** and noting that the request includes an IA token, the holder **201** uses the verifier's IA token to verify the identity of the verifier. The holder **201** may do this by, for example, by referencing information about the IA that is already in a local data store, or by lookup on the ledger to get the IA's information. If the IA token is from an identity authority that is known to the holder and the holder has a public key for the identity authority, then the holder may examine information in the IA token to determine whether the IA token has information indicating that the verifier may be trusted. If the IA token is from an identity authority that is known to the holder, but the holder does not have a public key for the identity authority, then the holder may look up the IA token on a distributed ledger or other service and examine information in the IA token accessed on the distributed ledger or other service. If the IA token is from an identity authority that is not known to the holder, then the holder may query an identity authority that is known to the holder as to whether the known identity authority has information indicating that the identity authority referenced by the verifier may be trusted.

[0041] Based on the result of the verification step (**312** or **322**), at **331** the holder **201** will determine whether or not verifier **203** is a trusted entity and thus legitimately allowed to

request the data. This step may be automated using internal data and programming logic, or the results may be presented to a human operator for manual decision and result determination based on the data that is presented.

[0042] If the verifier is determined to not be a trusted entity (**331: NO)**, then the holder rejects the request at **334** and no data is shared. If the verifier **203** is determined to be a trusted entity (**331: YES)**, then the holder accepts the request (either in full or for a subset of the data), and at **332** the holder **201** presents the requested data (or a subset of it) to the verifier **203.** As noted above, the requested data may be the issued data that the holder received from the issuer, or the requested data may be derived from the issued data.

[0043] At **332** the holder **201** will pass a proof to the verifier **203**. As illustrated in FIG. 6, the proof **612** will include one or more elements from one or more verifiable credentials **602**, where each element of the proof may be a copy of or derived through some computational process from, a corresponding element of the verifiable credential. The proof **612** will also contain evidence that each element is valid – i.e., was issued by the issuer to the holder and not tampered. The proof **612** also may include a signature provided by the holder **201** to prove that the holder is the one to whom the issuer provided the verifiable credential **602**. As illustrated in FIG. 2, the holder **201** may present the proof in response to a request from verifier **203**. For example, if the verifier **203** is part of or affiliated with an entity that provides a service, the verifier **203** may want to know that the issuer **202** authorized the holder **201** to access the service. Alternatively, the holder **201** may automatically pass the proof to the verifier with the data that the verifier requested.

[0044] At **333**, upon receiving the data from the holder, the verifier **203** verifies that the issuer information in the proof was actually from the issuer claimed in the proof (or derived from

information that the issuer issued) and not modified or tampered. At **340** the verifier **203** examines the credential for an IA token to assess whether the issuer can be trusted. If the credential contains one or more IA tokens (**340: YES**), then at **342** the verifier can use each IA token to get identifying information about the issuer referenced in the token, either directly from the identity authority **205** or by verification on the ledger **204**, even if the issuer **202** was not previously known to the verifier **203**. If the IA token is from an identity authority that is known to the verifier and the verifier has a public key for the identity authority, then the verifier may examine information in the IA token to determine whether the IA token has information indicating that the issuer may be trusted. If the IA token is from an identity authority that is known to the verifier but the verifier does not have a public key for the identity authority, then the verifier may look up the IA token on a distributed ledger and examine information in the IA token accessed on the distributed ledger. If the IA token is from an identity authority that is not known to the verifier, then the verifier may query an identity authority that is known to the verifier as to whether it has information indicating that the identity authority referenced by in the proof may be trusted.

[0045] If the proof references one or more issuers for which no IA token is included (**340: NO)**, then at **341** the verifier can use the issuer's DID in the credential to acquire the token (or the equivalent), either by a lookup on the ledger and using information in the IA token to determine whether to trust the issuer, or by a direct request to a known identity authority **205** to return information (such as a human-readable name or URL) that the verifier may use to determine whether to trusts the issuer.

[0046] At **350**, the verifier **203** uses the information from steps **340-342** to decide whether or not to trust the data received. If the verifier **203** is able to verify the issuer in either step **341** or **342**, then the verifier may determine that the proof was authorized by an issuer that is

a trusted entity (**350: YES**), and at **351** the verifier may accept the proof offered by the holder and use the holder's data for the requested purpose. For example, the verifier **203** may use the data to grant the holder access to a service, fill out a form for the holder, verify that the holder is (or is associated with) a person who is over a certain age, etc. If the verifier **203** does not verify the issuer in either step **341** or **342**, then the verifier will not determine that the proof was authorized by an issuer that is a trusted entity (**350: NO**), and at **321** the verifier may reject the offer and not use the holder's data for the requested purpose unless the data is verified by some other means.

[0047] An example use case for the digital identity solutions described in this document, a government agency may be able use the system to validate and store HIRE (household, income, resources, expenses) data in an applicant's digital vault. The applicant (i.e., the holder) will only share the data with the agency (the verifier) after confirming that the agency is a trusted entity. The applicant can then confidently share required pieces of data with an agency when applying for a program, and the agency can trust this data based on verifiable proofs using the blockchain/distributed ledger. For any new information received, the agency can verify that data and add the verified data back to the applicant's digital vault by acting as an issuer to write a verifiable credential containing this data.

[0048] As another example, an individual applicant may apply to an agency that is administering a food or cash assistance program. The individual may use the identity verification and data storage application on their mobile electronic device to create a user profile. The verifier, another entity, and/or the electronic device may require the user to associate identity verification information with the application. Such identity verification information may include, for example, a username and passcode, or a biometric identifier (such as fingerprint, voice print,

or facial recognition). The system also may verify that the user corresponds to a real, living person as stored in verifiable public records. The user may enter personally identifiable information such as that described in FIG. 7 above into the application, thus creating a secure digital vault for that information on the user's device, or on a server in a profile record that is only accessible to the application stored on the user's device. The user can then apply to various agencies for assistance, and upon notification that an agency website is that of a trusted entity, choose which information from the vault to share with that agency.

[0049] In this document, the terms "distributed ledger" and "digital ledger" each refer to an immutable data structure that is accessible by all participants in a transaction. An example is a blockchain, which includes a sequence of blocks that are linked together via nodes, and in which the blocks are replicated and distributed across multiple computing systems. In certain embodiments, a block may include a grouping of data or data records. Each block of a blockchain will include a link to an immediately preceding block in the blockchain, an immediately subsequent block in the blockchain, or both. Each block stores an identifier of its immediately preceding block, so that if the chain is broken or a block is inserted into the chain, the break or insertion will be detectable because of the mismatch of block data.

[0050] FIG. 8 illustrates an example blockchain data structure according to an embodiment. A blockchain **800a-N** includes one or more blocks **802a-N**. Optionally, a block may include one or more log records **804a-N**. As new log records are generated, a corresponding data representation of those log records may be added to the blockchain **800a-N** as part of a new block. As such, blocks **802a-N** of a blockchain **800a-N** may be positioned in a linear, sequential order. For example, blocks may be arranged in a chronological order. Blocks **802a-N** in a blockchain **800a-N** are linked to preceding blocks in the chain as illustrated in FIG. 8.

[0051] Optionally, one or more blocks **802a-N** of a blockchain **800a-N** may occupy the same data store or memory space. Alternatively, a blockchain **800a-N** may be implemented as or via a distributed data store. For instance, blocks **802a-N** of a blockchain **800a-N** may not occupy the same data store or memory space, but rather two or more blocks in a blockchain may be implemented as distributed data stores. These distributed data stores may exist amongst remote electronic devices. For instance, part of a blockchain **800a-N** may be stored in a data store that is associated with a first electronic device in a first location, while a different part of the blockchain may be stored in a different data store that is associated with a second electronic device in a second location that is different from the first location.

[0052] A block **802a-N** of a blockchain **800a-N** may be located in a data store at a first location, while a second block of the blockchain may be located in a data store at a second location. Despite remote storage proximity to one another, the blocks **802a-N** may still form the blockchain **800a-N** as they are linked to one another such as, for example, by way of their signatures.

[0053] When a blockchain infrastructure device receives a record (referred to in this document as a transaction record), that device or another device of the blockchain platform will bundle the transaction record with one or more other records into a block. When grouping the transaction record into a block, the system may choose a group of records having a total size that is within a target size range. The platform may apply any other set of rules to determine which records to group into a block, such as rules that prioritize certain types of records over others, or rules that will group records having one or more common attributes.

[0054] The blockchain platform will verify the transaction and/or validate the block and, upon verification and verification, add the block to the platform's permanent distributed digital ledger. To validate a transaction (which is a process that the system may do before or after

adding the transaction to a block), the system also may check the transaction against various rules. The rules can be kept on centralized servers, while in more distributed systems, all nodes that store any part of the blockchain would have a copy of all rules. For example, to validate a block, the system may create a proof of work for the block using any of various methods, such as by adding a nonce (a random number) to the block data, then hashing the block data. If the hash fails to meet the requirements of the proof of work, the nonce is changed and a new hash is made. When the system has successfully created a proof of work for a valid block, it sends the solution (the proof of work) to all nodes of the system.

[0055] FIG. 9 depicts an example of internal hardware that may be included in any of the electronic components of the system, such as the user's smartphone or a local or remote computing device in the system. An electrical bus **900** serves as an information highway interconnecting the other illustrated components of the hardware. Processor **905** is a central processing device of the system, configured to perform calculations and logic operations required to execute programming instructions. As used in this document and in the claims, the terms "processor" and "processing device" may refer to a single processor or any number of processors in a set of processors that collectively perform a set of operations, such as a central processing unit (CPU), a graphics processing unit (GPU), a remote server, or a combination of these. Read only memory (ROM), random access memory (RAM), flash memory, hard drives and other devices capable of storing electronic data constitute examples of memory devices **925**. A memory device may include a single device or a collection of devices across which data and/or instructions are stored.

[0056] An optional display interface **930** may permit information from the bus **900** to be displayed on a display device **935** in visual, graphic or alphanumeric format. An audio interface and audio output (such as a speaker) also may be provided. Communication with external devices

may occur using various communication devices **940** such as a wireless antenna, a radio frequency identification (RFID) tag and/or short-range or near-field communication transceiver, each of which may optionally communicatively connect with other components of the device via one or more communication systems. The communication device **940** may be configured to be communicatively connected to a communications network, such as the Internet, a local area network or a cellular telephone data network.

[0057] The hardware may also include a user interface sensor **945** that allows for receipt of data from input devices **950** such as a keyboard, a mouse, a joystick, a touchscreen, a touch pad, a remote control, a pointing device and/or microphone. Digital image frames also may be received from a camera **920** that can capture video and/or still images. The system also may include a positional sensor **990** and/or motion sensor **980** to detect position and movement of the device. Examples of motion sensors **880** include gyroscopes or accelerometers. Examples of positional sensors **990** include a global positioning system (GPS) sensor device that receives positional data from an external GPS network.

[0058] Terminology that is relevant to this disclosure includes:

[0059] An "electronic device" or a "computing device" refers to a device or system that includes a processor and memory. Each device may have its own processor and/or memory, or the processor and/or memory may be shared with other devices as in a virtual machine or container arrangement. The memory will contain or receive programming instructions that, when executed by the processor, cause the electronic device to perform one or more operations according to the programming instructions. Examples of electronic devices include, with reference to FIG. 1, personal computers **101**, servers **108 and 141a-n**, mainframes, virtual machines, containers, gaming systems, televisions, digital home assistants **102** and mobile

electronic devices such as smartphones **106**, fitness tracking devices, wearable virtual reality devices, Internet-connected wearables such as smart watches **104** and smart eyewear, personal digital assistants, cameras, tablet computers **103, 107**, laptop computers **105**, media players and the like. Electronic devices also may include appliances and other devices that can communicate in an Internet-of-things arrangement, such as smart thermostats, refrigerators, connected light bulbs and other devices. Electronic devices also may include components of vehicles such as dashboard entertainment and navigation systems, as well as on-board vehicle diagnostic and operation systems. In a client-server arrangement, the client device and the server are electronic devices, in which the server contains instructions and/or data that the client device accesses via one or more communications links in one or more communications networks. In a virtual machine arrangement, a server may be an electronic device, and each virtual machine or container also may be considered an electronic device. In the discussion above, a client device, server device, virtual machine or container may be referred to simply as a "device" for brevity. Additional elements that may be included in electronic devices are discussed above in the context of FIG. 9.

[0060] In this document, the terms "processor" and "processing device" refer to a hardware component of an electronic device that is configured to execute programming instructions. Except where specifically stated otherwise, the singular terms "processor" and "processing device" are intended to include both single-processing device embodiments and embodiments in which multiple processing devices together or collectively perform a process.

[0061] The terms "memory," "memory device," "computer-readable medium," "data store," "data storage facility" and the like each refer to a non-transitory device on which computer-readable data, programming instructions or both are stored. Except where specifically stated

otherwise, the terms “memory,” “memory device,” “computer-readable medium,” “data store,” “data storage facility” and the like are intended to include single device embodiments, embodiments in which multiple memory devices together or collectively store a set of data or instructions, as well as individual sectors within such devices. A computer program product is a memory device with programming instructions stored on it.

[0062] In this document, the terms “communication link” and “communication path” mean a wired or wireless path via which a first device sends communication signals to and/or receives communication signals from one or more other devices. Devices are “communicatively connected” if the devices are able to send and/or receive data via a communication link. “Electronic communication” refers to the transmission of data via one or more signals between two or more electronic devices, whether through a wired or wireless network, and whether directly or indirectly via one or more intermediary devices.

[0063] In this document, the term “electrically connected”, when referring to two electrical components, means that a conductive path exists between the two components. The term “communicatively connected”, when referring to two devices, means that a communication path exists between the two components. In either case, the path may be a direct path, or an indirect path through one or more intermediary components.

[0064] Without excluding further possible embodiments, certain example embodiments are summarized in the following statements:

[0065] Statement 1: In some embodiments, a method of verifying whether to share information with an entity comprises, by an electronic device of a holder (i) receiving a data request from an electronic device of a verifier; (ii) determining whether the verifier is a trusted entity by: (a) if the data request includes an identity authority (IA) token, using the IA token to

determine whether the verifier is a trusted entity, and (b) if the data request does not include the IA token, using a decentralized identifier (DID) for the verifier that was included in the data request to determine whether the verifier is a trusted entity; and (iii) upon determining that the verifier is a trusted entity, providing data to the verifier in response to the data request, otherwise rejecting the data request.

[0066] Statement 2: The method of statement 1 wherein, when the data request does not include the IA token, using the DID for the verifier to determine whether the verifier is a trusted entity comprises using the DID to either: (a) look up the IA token for the verifier on a distributed ledger and use information in the IA token to determine whether to trust the verifier; or (b) send the DID to a trusted IA to respond with information that the holder uses to determine whether to trust the verifier.

[0067] Statement 3: The method of statement 1 or 2 wherein, when the data request includes the IA token, using the IA token to determine whether the verifier is a trusted entity comprises: (a) if the IA token is from an IA that is known to the holder and the holder has a public key for the IA, examining information in the IA token to determine whether it has information indicating that the verifier may be trusted; (b) if the IA token is from an IA that is known to the holder, but the holder does not have a public key for the IA, looking up the IA token on a distributed ledger and examining information in the IA token accessed on the distributed ledger; or (c) if the IA token is from an IA that is not known to the holder, querying an IA that is known to the holder as to whether it has information enabling the verifier to determine whether or not the IA associated with the IA token in the proof may be trusted.

[0068] Statement 4: The method of any of statements 1-3 further comprising, by the holder electronic device, receiving, from an electronic device of an issuer: (a) a verifiable

credential that comprises an issuer DID, an issuer signature, an IA DID, and an IA signature; and (b) issued data, wherein the issued data may or may not be included within the credential.

[0069] Statement 5: The method of statement 4 further comprising, by the holder electronic device, providing a proof to the verifier in response to the data request, wherein the proof comprises elements that are, or that are derived from, elements of the verifiable credential.

[0070] Statement 6: The method of statement 4 or 5, wherein the data provided to the verifier comprises the issued data and/or is derived from the issued data.

[0071] Statement 7: In some embodiments, a method of verifying whether to trust information received from an entity comprises, by an electronic device of a verifier: (i) sending a data request to an electronic device of a holder; (ii) in response, receiving data and a proof from the holder, wherein the proof comprises a decentralized identifier (DID) and a signature of an issuer; (iii) determining whether the data is associated with a trusted issuer by: (a) examining the proof to determine whether the proof also includes an identity authority (IA) token, (b) if the proof includes an IA token that was issued by a known IA, using the IA token to determine whether the issuer is a trusted entity, (c) if the proof does not include the IA token, using the DID for the issuer that is in the proof to determine whether the issuer is a trusted entity; and (d) if the IA token is from an IA that is not known to the holder, querying an IA that is known to the holder as to whether it has information enabling the verifier to determine whether or not the IA associated with the IA token in the proof may be trusted.

[0072] and (iv) upon determining that the issuer is a trusted entity, accepting the proof and using the data, otherwise rejecting the proof and the data.

[0073] Statement 8: The embodiment of statement 7 may be combined with any of statements 1-6.

[0074] Statement 9: The method of statement 7 or 8 wherein, when the credential does not include the IA token, using the DID for the issuer to determine whether the issuer is a trusted entity comprises using the DID to look up the IA token for the issuer on a distributed ledger and use information in the IA token to determine whether to trust the issuer, or to send the DID request to a trusted IA to respond with information that the holder uses to determine whether to trust the issuer.

[0075] Statement 10: The method of any of statements 7-9 wherein, when the credential includes the IA token, using the IA token to determine whether the issuer is a trusted entity comprises: (a) if the IA token is from an IA that is known to the verifier and the verifier has a public key for the IA, examining information in the IA token to determine whether the IA token has information indicating that the issuer may be trusted; (b) if the IA token is from an IA that is known to the verifier but the verifier does not have a public key for the IA, looking up the IA token on a distributed ledger and examining information in the IA token accessed on the distributed ledger; or (c) if the IA token is from an IA that is not known to the verifier, querying an IA that is known to the verifier as to whether it has information enabling the verifier to determine whether or not the IA associated with the IA token in the proof may be trusted.

[0076] Statement 11: The method of any of statements 7-10 wherein the data is included within the proof.

[0077] Statement 12: The method of any of statements 7-11 further comprising, by the issuer before the verifier sends the data request to the electronic device of the holder: (a) writing the DID for the issuer to a distributed ledger; (b) presenting the DID for the issuer to the known IA in a request for the IA token from the known IA; and (c) writing the DID for the issuer to a distributed ledger.

[0078] Statement 13: The method of statement 12 further comprising, by the issuer, presenting the holder with a credential that includes the DID for the issuer and the signature of the issuer.

[0079] The features and functions described above, as well as alternatives, may be combined into many other different systems or applications. Various alternatives, modifications, variations or improvements may be made by those skilled in the art, each of which is also intended to be encompassed by the disclosed embodiments.

CLAIMS

1. A method of verifying whether to share information with an entity, the method comprising, by an electronic device of a holder:

receiving a data request from an electronic device of a verifier;

determining whether the verifier is a trusted entity by:

if the data request includes an identity authority (IA) token, using the IA token to determine whether the verifier is a trusted entity, and

if the data request does not include the IA token, using a decentralized identifier (DID) for the verifier that was included in the data request to determine whether the verifier is a trusted entity; and

upon determining that the verifier is a trusted entity, providing data to the verifier in response to the data request, otherwise rejecting the data request.

2. The method of claim 1 wherein, when the data request does not include the IA token, using the DID for the verifier to determine whether the verifier is a trusted entity comprises using the DID to either:

look up the IA token for the verifier on a distributed ledger and use information in the IA token to determine whether to trust the verifier; or

send the DID to a trusted IA to respond with information that the holder uses to determine whether to trust the verifier.

3. The method of claim 1 wherein, when the data request includes the IA token, using the IA token to determine whether the verifier is a trusted entity comprises:

if the IA token is from an IA that is known to the holder and the holder has a public key for the IA, examining information in the IA token to determine whether it has information indicating that the verifier may be trusted;

if the IA token is from an IA that is known to the holder, but the holder does not have a public key for the IA, looking up the IA token on a distributed ledger and examining information in the IA token accessed on the distributed ledger; or

if the IA token is from an IA that is not known to the holder, querying an IA that is known to the holder as to whether it has information enabling the verifier to determine whether or not the IA associated with the IA token in the proof may be trusted.

4. The method of claim 1 further comprising, by the holder electronic device:

receiving, from an electronic device of an issuer:

a verifiable credential that comprises an issuer DID, an issuer signature, an IA DID, and an IA signature; and

issued data, wherein the issued data is or is not included within the credential.

5. The method of claim 4 further comprising, by the holder electronic device, providing a proof to the verifier in response to the data request, wherein the proof comprises elements that are, or that are derived from, elements of the verifiable credential.

6. The method of claim 4, wherein the data provided to the verifier comprises the issued data and/or is derived from the issued data.

7. The method of claim 1 further comprising, by an electronic device of a verifier:

sending a data request to an electronic device of the holder;

receiving data and a proof from the holder, wherein the proof comprises a DID and a signature of an issuer;

determining whether the data is associated with a trusted issuer by:

examining the proof to determine whether the proof also includes the IA token,

if the proof includes the IA token, using the IA token to determine whether the issuer is a trusted entity, and

if the proof does not include the IA token, using the DID for the issuer that is in the proof to determine whether the issuer is a trusted entity; and

upon determining that the issuer is a trusted entity, accepting the proof and using the data, otherwise rejecting the proof and the data.

8. A computer program product comprising a memory device and programming instructions that are configured to cause a processor of an electronic device of a holder to perform a method of verifying whether to share information with an entity, the method comprising:

receiving a data request from an electronic device of a verifier;

determining whether the verifier is a trusted entity by:

if the data request includes an identity authority (IA) token, using the IA token to determine whether the verifier is a trusted entity, and

if the data request does not include the IA token, using a decentralized identifier (DID) for the verifier that was included in the data request to determine whether the verifier is a trusted entity; and

upon determining that the verifier is a trusted entity, providing data to the verifier in response to the data request, otherwise rejecting the data request.

9. The computer program product of claim 8, further comprising further comprising programming instructions that are configured to cause an electronic device of a verifier to perform a method comprising:

sending a data request to an electronic device of the holder;

receiving data and a proof from the holder, wherein the proof comprises a DID and a signature of an issuer; and

determining whether the data is associated with a trusted issuer by:

examining the proof to determine whether the proof also includes the IA token,

if the proof includes the IA token, using the IA token to determine whether the issuer is a trusted entity, and

if the proof does not include the IA token, using the DID for the issuer that is in the proof to determine whether the issuer is a trusted entity; and

upon determining that the issuer is a trusted entity, accepting the proof and using the data, otherwise rejecting the proof and the data.

10. A method of verifying whether to trust information received from an entity, the method comprising, by an electronic device of a verifier:

sending a data request to an electronic device of a holder;

in response to the data request, receiving data and a proof from the holder, wherein the proof comprises a decentralized identifier (DID) and a signature of an issuer;

determining whether the data is associated with a trusted issuer by:

examining the proof to determine whether the proof also includes an identity authority (IA) token,

if the proof includes an IA token that was issued by a known IA, using the IA token to determine whether the issuer is a trusted entity,

if the proof does not include the IA token, using the DID for the issuer that is in the proof to determine whether the issuer is a trusted entity, and

if the IA token is from an IA that is not known to the holder, querying an IA that is known to the holder as to whether it has information enabling the verifier to determine whether or not the IA associated with the IA token in the proof may be trusted; and

upon determining that the issuer is a trusted entity, accepting the proof and using the data, otherwise rejecting the proof and the data.

11. The method of claim 10 wherein, when the proof does not include the IA token, using the DID for the issuer to determine whether the issuer is a trusted entity comprises using the DID to either:

look up the IA token for the issuer on a distributed ledger and use information in the IA token to determine whether to trust the issuer; or

send the DID request to a trusted IA to respond with information that the verifier uses to determine whether to trust the issuer.

12. The method of claim 10 wherein, when the credential includes the IA token, using the IA token to determine whether the issuer is a trusted entity comprises:

if the IA token is from an IA that is known to the verifier and the verifier has a public key for the IA, examining information in the IA token to determine whether the IA token has information indicating that the issuer may be trusted;

if the IA token is from an IA that is known to the verifier but the verifier does not have a public key for the IA, looking up the IA token on a distributed ledger and examining information in the IA token accessed on the distributed ledger; or

if the IA token is from an IA that is not known to the verifier, querying an IA that is known to the verifier as to whether it has information enabling the verifier to determine whether or not the IA associated with the IA token in the proof may be trusted.

13. The method of claim 10, wherein the data is included within the proof.

14. The method of claim 10 further comprising, by the issuer before the verifier sends the data request to the electronic device of the holder:

writing the DID for the issuer to a distributed ledger;

presenting the DID for the issuer to the known IA in a request for the IA token from the known IA; and

receiving the IA token from the known IA in response to the request for the IA token.

15. The method of claim 14 further comprising, by the issuer, presenting the holder with a credential that includes the DID for the issuer and the signature of the issuer.

16. A computer program product comprising a memory device and programming instructions that are configured to cause a processor of an electronic device of a verifier to perform a method of determining whether to trust information received from with an entity, the method comprising:

sending a data request to an electronic device of a holder;

in response to the data request, receiving data and a proof from the holder, wherein the proof comprises a decentralized identifier (DID) and a signature of an issuer; and

determining whether the data is associated with a trusted issuer by:

examining the proof to determine whether the proof also includes an identity authority (IA) token,

if the proof includes an IA token that was issued by a known IA, using the IA token to determine whether the issuer is a trusted entity, and

if the proof does not include the IA token, using the DID for the issuer that is in the proof to determine whether the issuer is a trusted entity; and

upon determining that the issuer is a trusted entity, accepting the proof and using the data, otherwise rejecting the proof and the data.

17. The computer program product of claim 16, further comprising programming instructions that are configured to cause an electronic device of the holder to:

present the DID for the issuer to the known IA in a request for the IA token from the known IA;

receive the IA token from the known IA in response to the request for the IA token; and

write the DID for the issuer to a distributed ledger.

18. The computer program product of claim 17, further comprising programming instructions that are configured to cause an electronic device of a verifier to perform a method comprising:

sending a data request to an electronic device of the holder;

in response to the data request, receiving data and a proof from the holder, wherein the proof comprises a DID and a signature of an issuer; and

determining whether the data is associated with a trusted issuer by:

examining the proof to determine whether the proof also includes the IA token,

if the proof includes the IA token, using the IA token to determine whether the issuer is a trusted entity, and

if the proof does not include the IA token, using the DID for the issuer that is in the proof to determine whether the issuer is a trusted entity; and

upon determining that the issuer is a trusted entity, accepting the proof and using the data, otherwise rejecting the proof and the data.

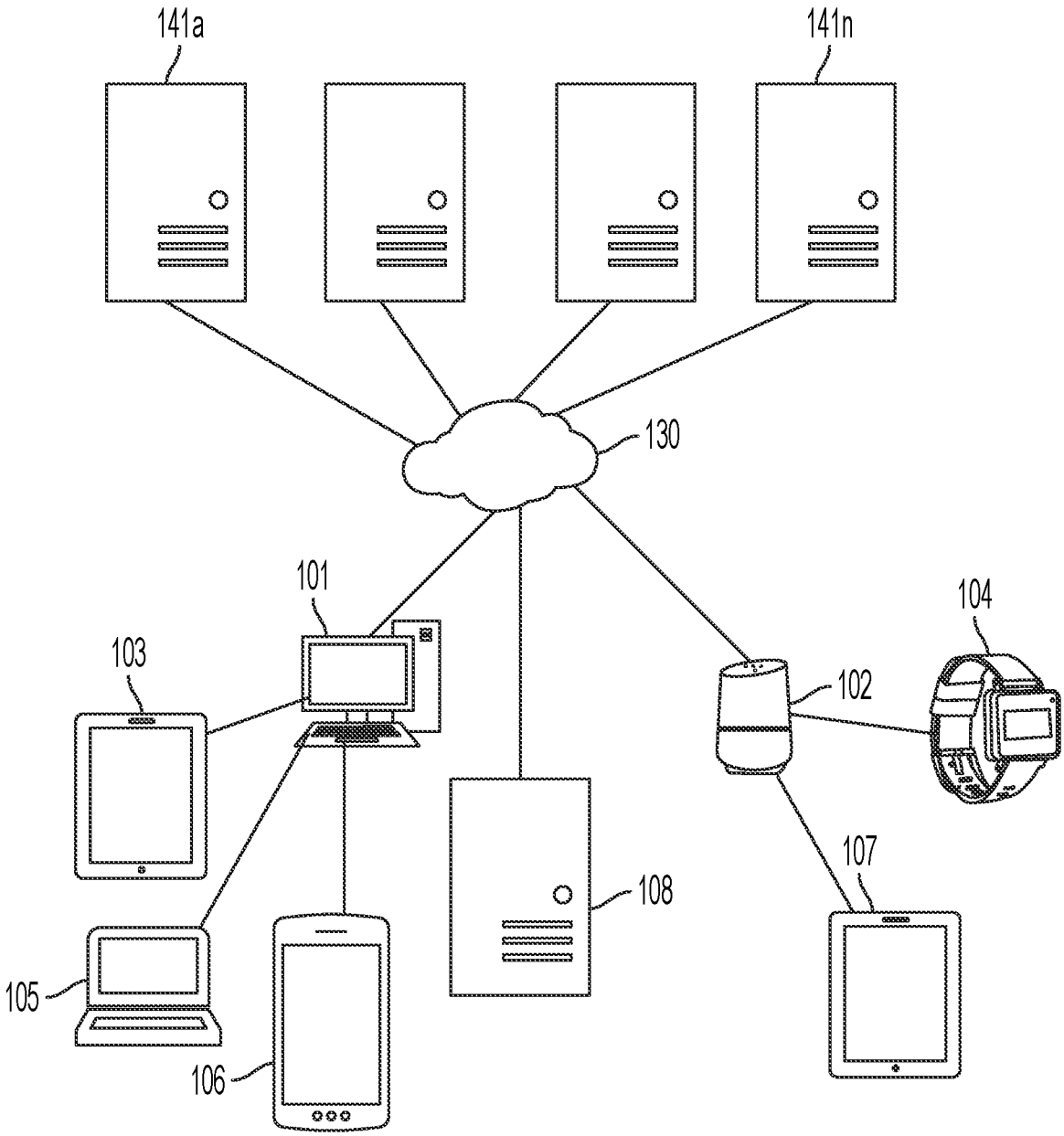

FIG. 1

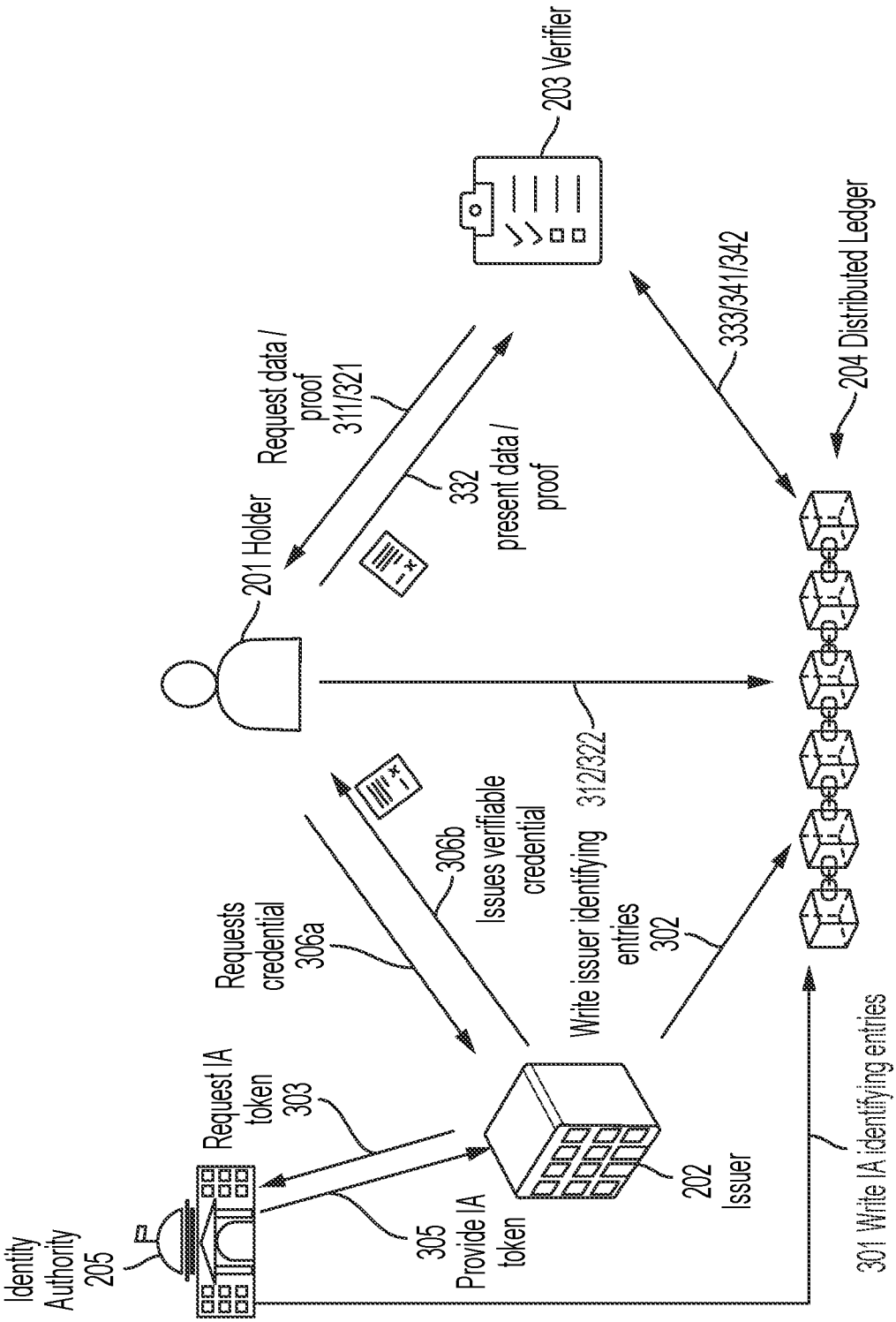
Identity Authority 205
Request IA token 303
305 Provide IA token
202 Issuer
301 Write IA identifying entries
Requests credential 306a
306b Issues verifiable credential
Write issuer identifying entries 302
312/322
201 Holder
Request data / proof 311/321
332 present data / proof
203 Verifier
333/341/342
204 Distributed Ledger

FIG. 2

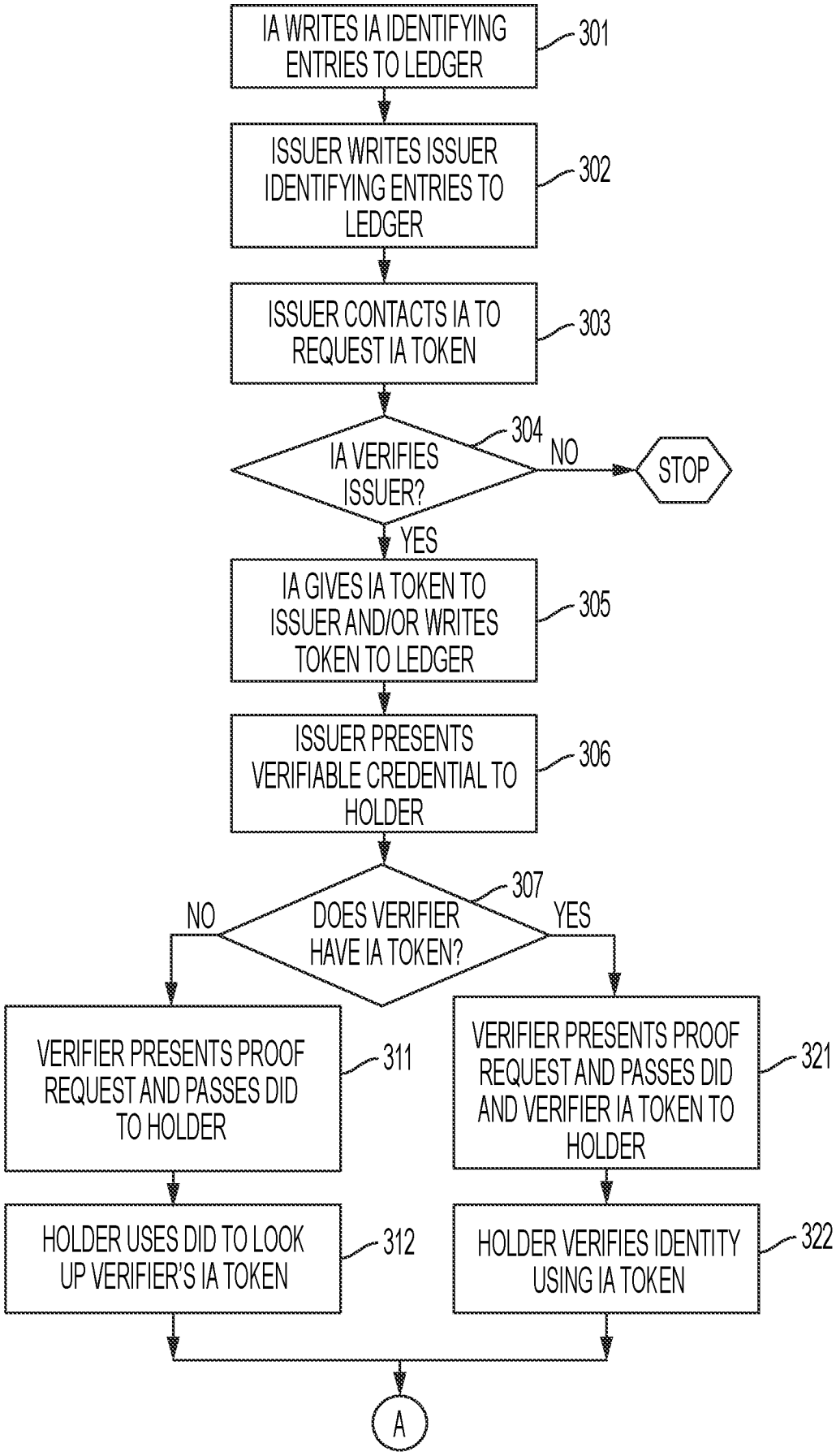
IA WRITES IA IDENTIFYING ENTRIES TO LEDGER
301
ISSUER WRITES ISSUER IDENTIFYING ENTRIES TO LEDGER
302
ISSUER CONTACTS IA TO REQUEST IA TOKEN
303
IA VERIFIES ISSUER?
304
NO
STOP
YES
IA GIVES IA TOKEN TO ISSUER AND/OR WRITES TOKEN TO LEDGER
305
ISSUER PRESENTS VERIFIABLE CREDENTIAL TO HOLDER
306
DOES VERIFIER HAVE IA TOKEN?
307
NO
YES
VERIFIER PRESENTS PROOF REQUEST AND PASSES DID TO HOLDER
311
VERIFIER PRESENTS PROOF REQUEST AND PASSES DID AND VERIFIER IA TOKEN TO HOLDER
321
HOLDER USES DID TO LOOK UP VERIFIER'S IA TOKEN
312
HOLDER VERIFIES IDENTITY USING IA TOKEN
322
A

FIG. 3A

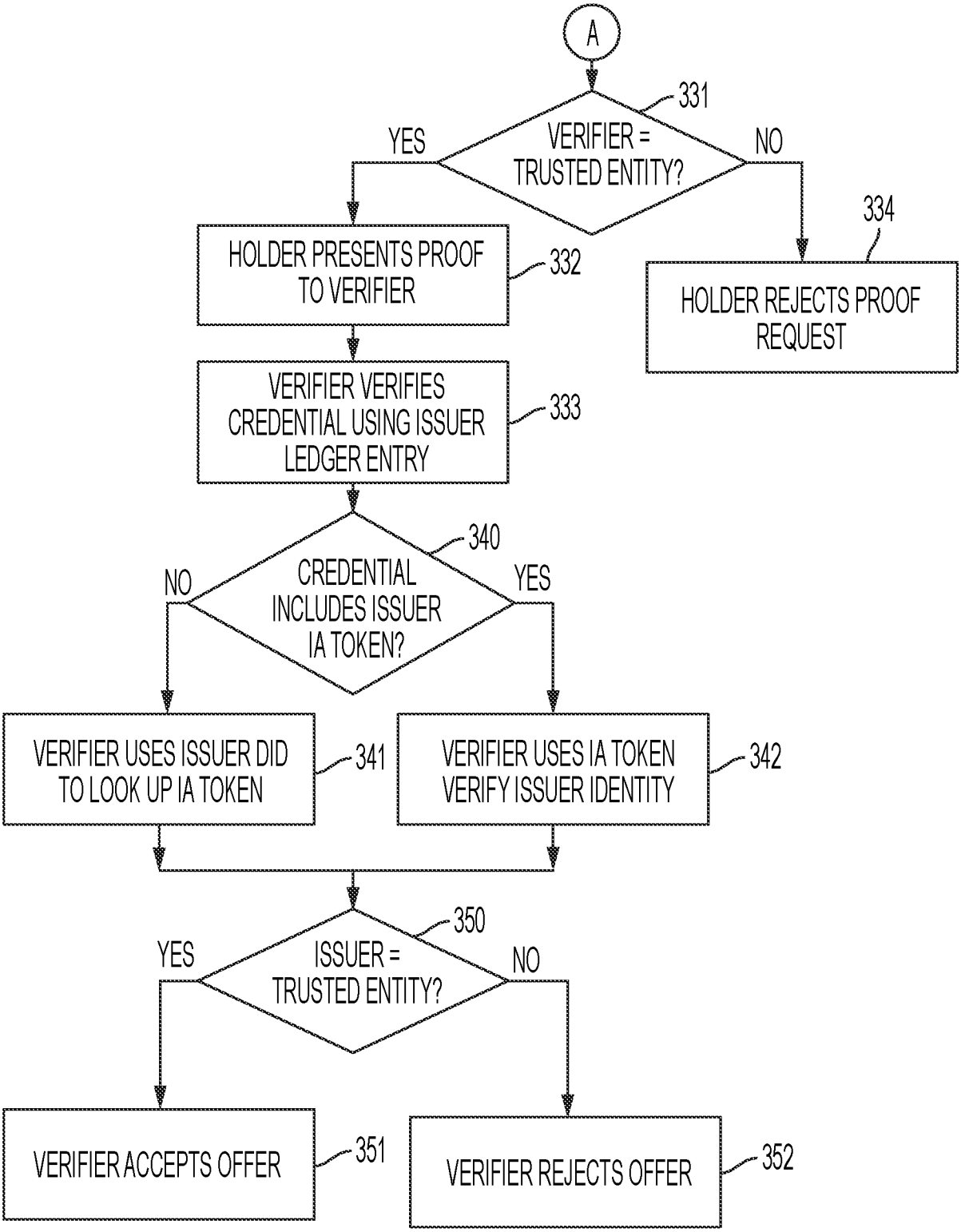
A
331
VERIFIER = TRUSTED ENTITY?
YES
NO
334
HOLDER PRESENTS PROOF TO VERIFIER
332
HOLDER REJECTS PROOF REQUEST
VERIFIER VERIFIES CREDENTIAL USING ISSUER LEDGER ENTRY
333
340
CREDENTIAL INCLUDES ISSUER IA TOKEN?
NO
YES
VERIFIER USES ISSUER DID TO LOOK UP IA TOKEN
341
VERIFIER USES IA TOKEN VERIFY ISSUER IDENTITY
342
350
ISSUER = TRUSTED ENTITY?
YES
NO
VERIFIER ACCEPTS OFFER
351
VERIFIER REJECTS OFFER
352

FIG. 3B

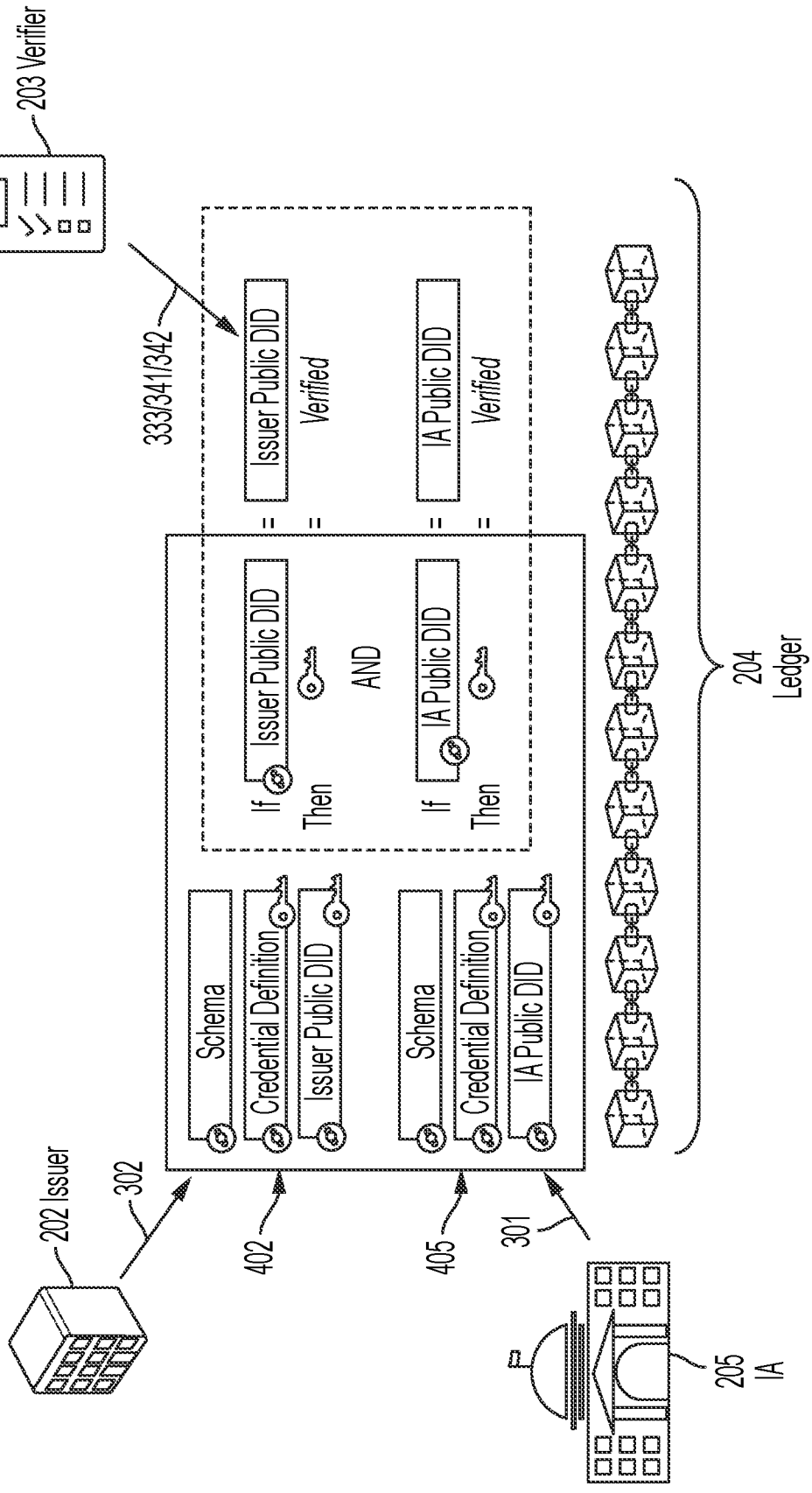
203 Verifier
333/341/342
Issuer Public DID
Verified
IA Public DID
Verified
If
Then
Issuer Public DID
AND
If
Then
IA Public DID
Schema
Credential Definition
Issuer Public DID
Schema
Credential Definition
IA Public DID
204
Ledger
202 Issuer
302
402
405
301
205
IA

FIG. 4

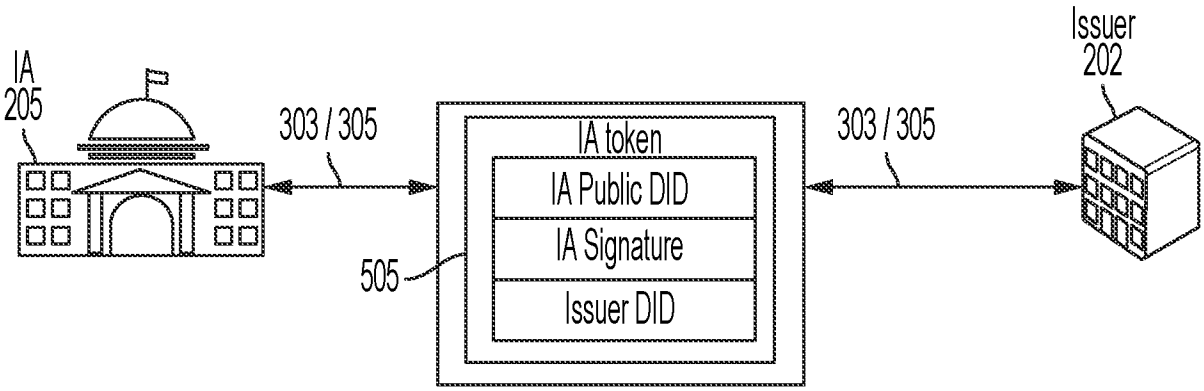
IA
205
303 / 305
IA token
IA Public DID
IA Signature
Issuer DID
505
303 / 305
Issuer
202

FIG. 5

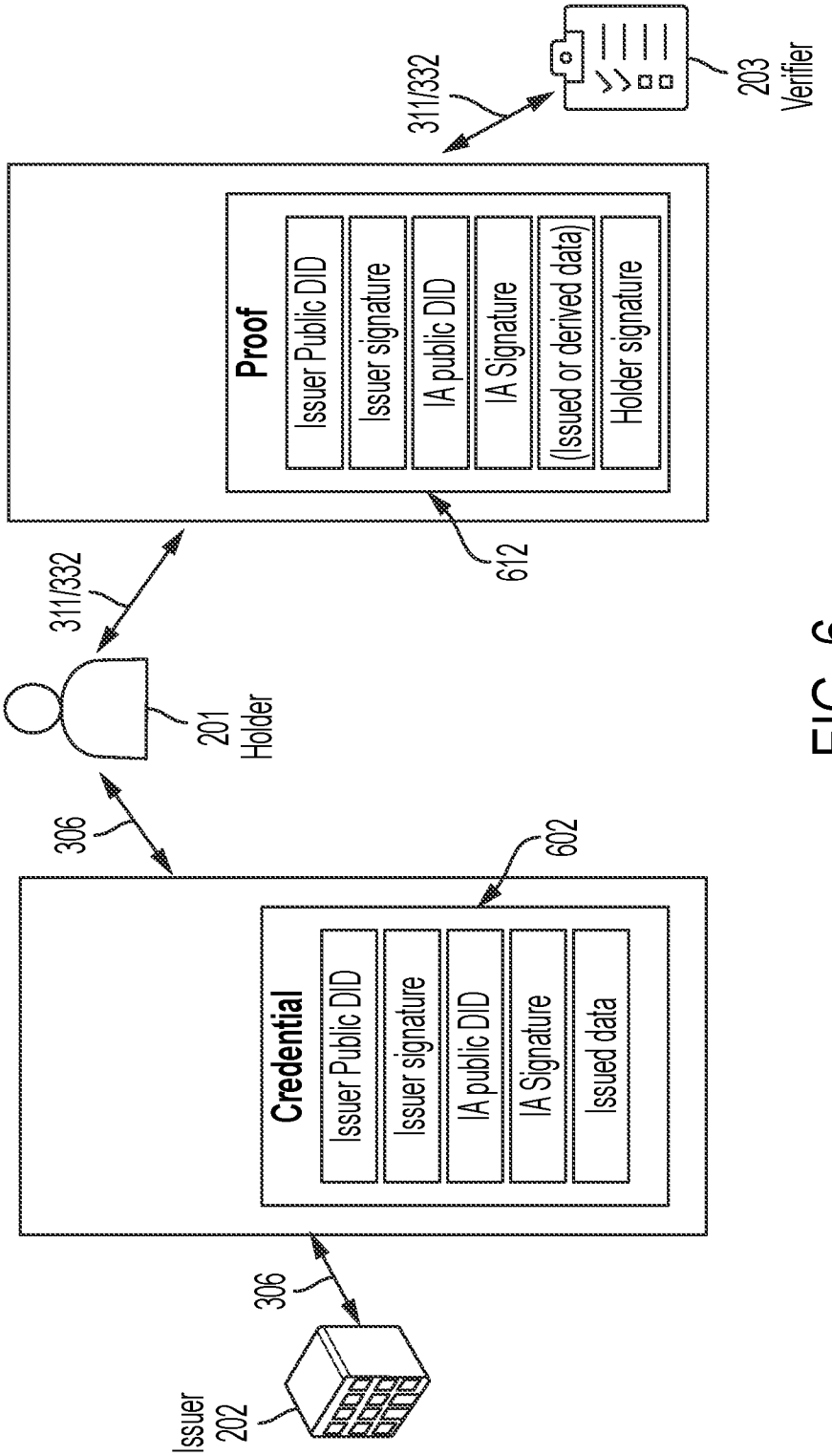
311/332
203
Verifier
Proof
Issuer Public DID
Issuer signature
IA public DID
IA Signature
(Issued or derived data)
Holder signature
612
311/332
201
Holder
306
602
Credential
Issuer Public DID
Issuer signature
IA public DID
IA Signature
Issued data
306
Issuer
202

FIG. 6

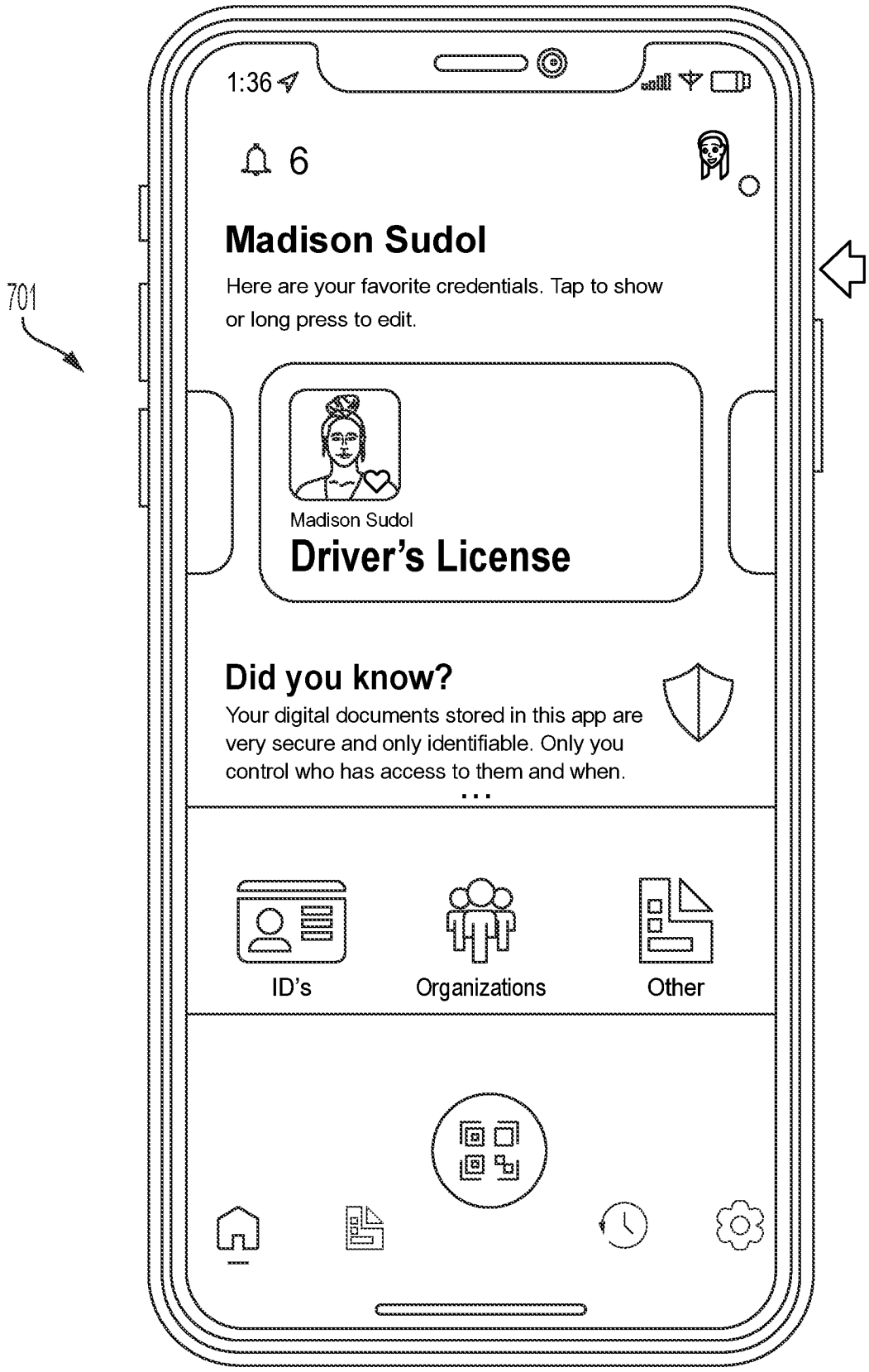
701
1:36
6
Madison Sudol
Here are your favorite credentials. Tap to show or long press to edit.
Madison Sudol
Driver's License
Did you know?
Your digital documents stored in this app are very secure and only identifiable. Only you control who has access to them and when.
ID's
Organizations
Other

FIG. 7

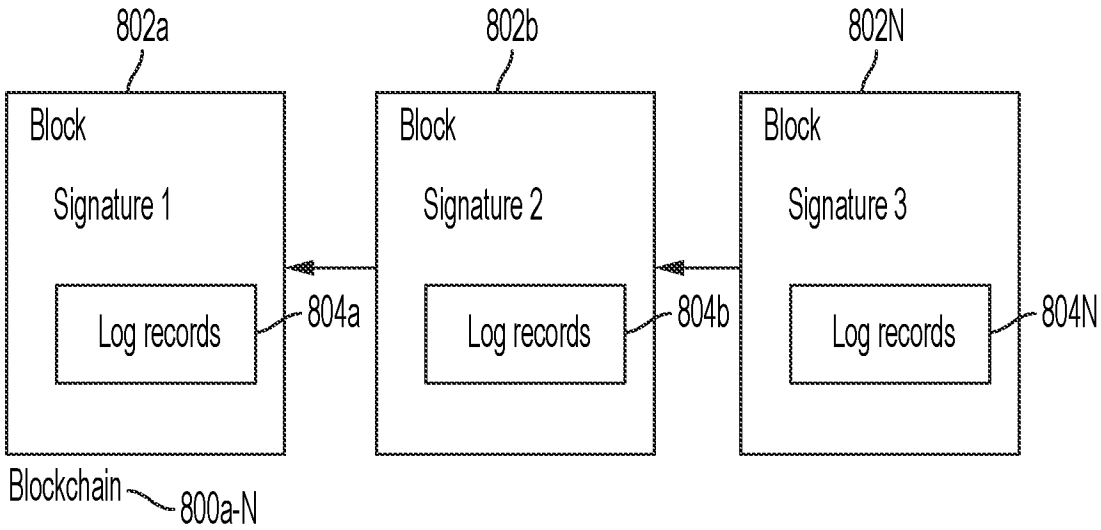
802a
802b
802N
Block
Signature 1
Log records
804a
Block
Signature 2
Log records
804b
Block
Signature 3
Log records
804N
Blockchain
800a-N

FIG. 8

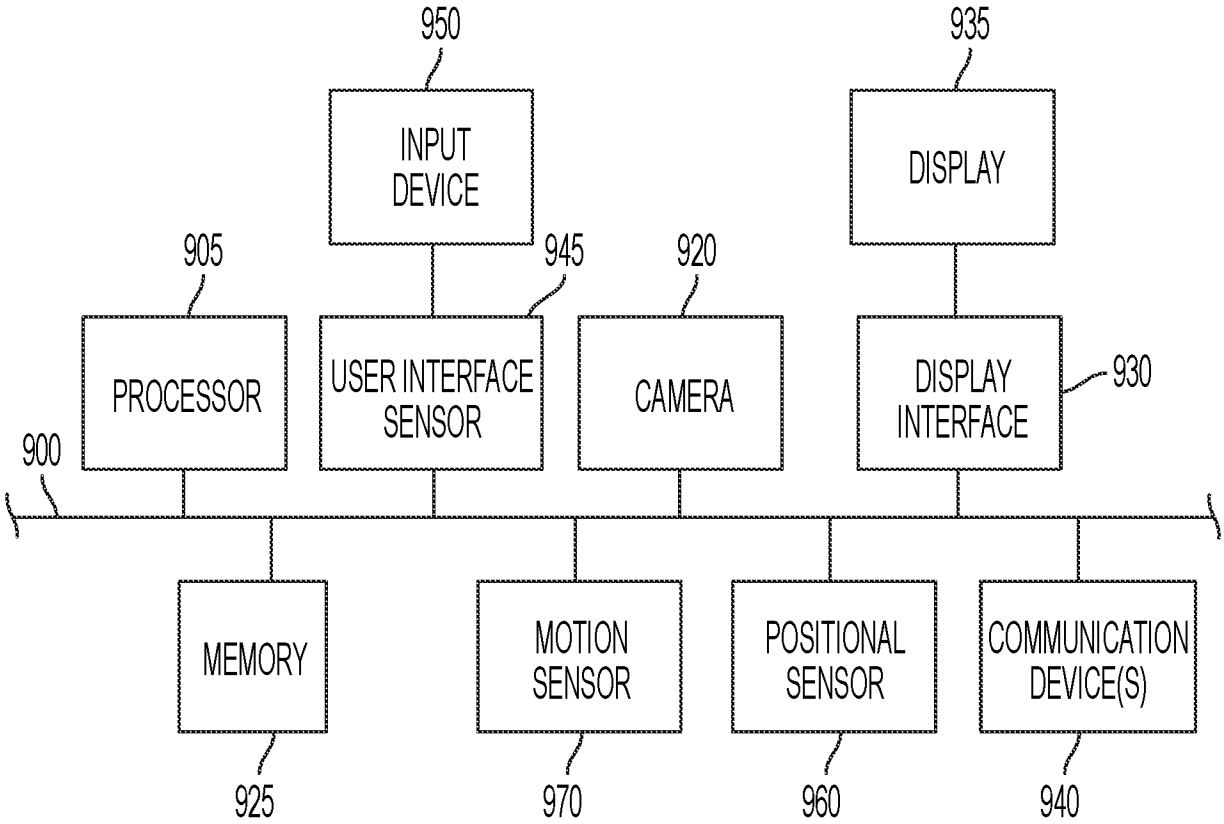
950
INPUT DEVICE
935
DISPLAY
905
945
920
PROCESSOR
USER INTERFACE SENSOR
CAMERA
DISPLAY INTERFACE
930
900
MEMORY
MOTION SENSOR
POSITIONAL SENSOR
COMMUNICATION DEVICE(S)
925
970
960
940

FIG. 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2023/060252

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/33(2023.01)i; ***G06Q 20/38***(2023.01)i; ***G06Q 20/40***(2023.01)i; ***G06Q 20/02***(2023.01)i; ***H04M 7/00***(2023.01)i; ***H04L 9/00***(2023.01)i; ***H04L 9/32***(2023.01)i; ***H04L 9/40***(2023.01)i
CPC:G06F 21/33; G06Q 20/38215; G06Q 20/4014; G06Q 20/02; H04M 7/0078; H04L 9/50; H04L 9/3236; H04L 63/08

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)

G06F 21/33; G06Q 20/38; G06Q 20/40; G06Q 20/02; H04M 7/00; H04L 9/00; H04L 9/32; H04L 9/40
CPC:G06F 21/33; G06Q 20/38215; G06Q 20/4014; G06Q 20/02; H04M 7/0078; H04L 9/50; H04L 9/3236; H04L 63/08

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)

Databases consulted: Orbit, Similari (AI-based)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2019207951 A1 (CAMBRIDGE BLOCKCHAIN INC [US]) 04 July 2019 (2019-07-04) The whole document	1-18
X	US 2021288974 A1 (MICROSOFT TECHNOLOGY LICENSING LLC [US]) 16 September 2021 (2021-09-16) The whole document	1-3,7-12,14-18
A	US 2020153639 A1 (ALIBABA GROUP HOLDING LTD [KY]) 14 May 2020 (2020-05-14) The whole document	1-18
A	US 2020274713 A1 (TBCASOFT INC [US]) 27 August 2020 (2020-08-27) The whole document	1-18
A	US 2020177377 A1 (CIVIC TECH INC [US]) 04 June 2020 (2020-06-04) The whole document	1-18
A	US 2017180128 A1 (GEMALTO INC [US]) 22 June 2017 (2017-06-22) The whole document	1-18

☐ 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
"D" document cited by the applicant in the international application
"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
06 March 2023	**26 March 2023**

Name and mailing address of the ISA/IL	Authorized officer
Israel Patent Office **Technology Park, Bldg.5, Malcha, Jerusalem, 9695101,** **Israel** **Israel** Telephone No. **972-73-3927126** Email: **pctoffice@justice.gov.il**	**NAIM Tal** Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2023/060252

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
US 2019207951 A1	04 July 2019	US 2019207951 A1	04 July 2019
		US 11212296 B2	28 December 2021
		CA 3002034 A1	20 April 2017
		CN 108701276 A	23 October 2018
		CN 108701276 B	12 April 2022
		DE 202016008801 U1	04 November 2019
		EP 3234878 A1	25 October 2017
		HK 1245468 A1	24 August 2018
		JP 2018537022 A	13 December 2018
		JP 6951329 B2	20 October 2021
		KR 20180108566 A	04 October 2018
		SG 11201803010U A	30 May 2018
		US 2017111175 A1	20 April 2017
		US 9667427 B2	30 May 2017
		US 2017222814 A1	03 August 2017
		US 9749140 B2	29 August 2017
		US 2018234433 A1	16 August 2018
		US 10938835 B2	02 March 2021
		US 2021352083 A1	11 November 2021
		WO 2017066715 A1	20 April 2017
US 2021288974 A1	16 September 2021	US 2021288974 A1	16 September 2021
		EP 4121879 A1	25 January 2023
		WO 2021188203 A1	23 September 2021
US 2020153639 A1	14 May 2020	US 2020153639 A1	14 May 2020
		US 10924284 B2	16 February 2021
		CN 111095865 A	01 May 2020
		CN 111164594 A	15 May 2020
		CN 111183426 A	19 May 2020
		CN 111213147 A	29 May 2020
		CN 111213350 A	29 May 2020
		CN 111213350 B	29 July 2022
		CN 111295869 A	16 June 2020
		CN 111295869 B	22 April 2022
		CN 111316303 A	19 June 2020
		CN 111373400 A	03 July 2020
		EP 3688634 A2	05 August 2020
		EP 3688634 A4	07 October 2020
		EP 3688634 B1	16 February 2022
		EP 3688930 A2	05 August 2020
		EP 3688930 A4	23 September 2020
		EP 3688930 B1	20 October 2021
		EP 3704620 A2	09 September 2020
		EP 3704620 A4	25 November 2020
		EP 3704620 B1	15 December 2021
		EP 3732856 A2	04 November 2020
		EP 3732856 A4	20 January 2021
		EP 3732856 B1	06 April 2022
		EP 3732857 A2	04 November 2020
		EP 3732857 A4	30 December 2020
		EP 3732857 B1	22 February 2023

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2023/060252

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
		EP	3788522	A1	10 March 2021
		EP	3788522	A4	10 March 2021
		EP	3788522	B1	30 November 2022
		EP	3788523	A1	10 March 2021
		EP	3788523	A4	10 March 2021
		EP	3788523	B1	16 March 2022
		EP	3814948	A1	05 May 2021
		EP	3814948	A4	01 December 2021
		EP	4016544	A1	22 June 2022
		SG	11202003757T	A	28 May 2020
		SG	11202003936W	A	25 February 2021
		SG	11202003946P	A	28 May 2020
		SG	11202004456T	A	29 June 2020
		SG	11202004850P	A	25 February 2021
		SG	11202005591S	A	25 February 2021
		SG	11202006574P	A	28 August 2020
		SG	11202006772Q	A	28 August 2020
		TW	202103033	A	16 January 2021
		TW	I721840	B	11 March 2021
		TW	202103029	A	16 January 2021
		TW	I725793	B	21 April 2021
		TW	202103036	A	16 January 2021
		TW	I737236	B	21 August 2021
		US	2020143019	A1	07 May 2020
		US	10685099	B2	16 June 2020
		US	2020145196	A1	07 May 2020
		US	10700851	B2	30 June 2020
		US	2020145223	A1	07 May 2020
		US	10708060	B2	07 July 2020
		US	2020145229	A1	07 May 2020
		US	10728042	B2	28 July 2020
		US	2020153606	A1	14 May 2020
		US	10756885	B2	25 August 2020
		US	2020242221	A1	30 July 2020
		US	10824701	B2	03 November 2020
		US	2020304315	A1	24 September 2020
		US	10917246	B2	09 February 2021
		US	2020244439	A1	30 July 2020
		US	10938551	B2	02 March 2021
		US	2021051025	A1	18 February 2021
		US	11025435	B2	01 June 2021
		US	2020328878	A1	15 October 2020
		US	11038670	B2	15 June 2021
		US	2020145209	A1	07 May 2020
		US	11038883	B2	15 June 2021
		US	2020127847	A1	23 April 2020
		US	11082233	B2	03 August 2021
		US	2021126916	A1	29 April 2021
		US	11159526	B2	26 October 2021
		US	2021111867	A1	15 April 2021

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2023/060252

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
				US	11171789	B2	09 November 2021
				US	2021351934	A1	11 November 2021
				US	11316697	B2	26 April 2022
				US	2021185041	A1	17 June 2021
				US	11477032	B2	18 October 2022
				US	2021075589	A1	11 March 2021
				US	11533164	B2	20 December 2022
				WO	2019179533	A2	26 September 2019
				WO	2019179533	A3	07 May 2020
				WO	2019179537	A2	26 September 2019
				WO	2019179537	A3	30 April 2020
				WO	2019228555	A2	05 December 2019
				WO	2019228555	A3	30 April 2020
				WO	2019228556	A2	05 December 2019
				WO	2019228556	A3	30 April 2020
				WO	2019228557	A2	05 December 2019
				WO	2019228557	A3	30 April 2020
				WO	2021000337	A1	07 January 2021
				WO	2021000419	A1	07 January 2021
				WO	2021000420	A1	07 January 2021
US	2020274713	A1	27 August 2020	US	2020274713	A1	27 August 2020
				CN	113853775	A	28 December 2021
				EP	3932002	A1	05 January 2022
				EP	3932002	A4	05 October 2022
				JP	2022531754	A	11 July 2022
				KR	20220002874	A	07 January 2022
				SG	11202109105W	A	29 September 2021
				WO	2020176691	A1	03 September 2020
US	2020177377	A1	04 June 2020	US	2020177377	A1	04 June 2020
				CA	3022628	A1	02 November 2017
				CN	109417549	A	01 March 2019
				CN	109417549	B	02 November 2021
				CN	114037435	A	11 February 2022
				EP	3449408	A1	06 March 2019
				EP	3449408	A4	25 December 2019
				US	2017317833	A1	02 November 2017
				US	10333705	B2	25 June 2019
				US	2017317834	A1	02 November 2017
				US	10333706	B2	25 June 2019
				US	2018255038	A1	06 September 2018
				US	10361849	B2	23 July 2019
				US	2019296904	A1	26 September 2019
				US	10558974	B2	11 February 2020
				US	2019280861	A1	12 September 2019
				US	10652018	B2	12 May 2020
				US	2017317997	A1	02 November 2017
				US	10666434	B2	26 May 2020
				US	2017316390	A1	02 November 2017
				US	2017316409	A1	02 November 2017
				US	2017316410	A1	02 November 2017

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2023/060252

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
		US 2018253703 A1	06 September 2018
		US 2018253724 A1	06 September 2018
		US 2018253725 A1	06 September 2018
		US 2018316507 A1	01 November 2018
		WO 2017190057 A1	02 November 2017
US 2017180128 A1	22 June 2017	US 2017180128 A1	22 June 2017
		US 10079682 B2	18 September 2018
		EP 3395006 A1	31 October 2018
		EP 3395006 B1	05 May 2021
		ES 2881289 T3	29 November 2021
		HK 1255142 A1	09 August 2019
		JP 2019506103 A	28 February 2019
		JP 2020145733 A	10 September 2020
		SG 11201804361Y A	30 July 2018
		US 2018359092 A1	13 December 2018
		US 10673632 B2	02 June 2020
		WO 2017108783 A1	29 June 2017