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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 January 2023 (19.01.2023)

WIPO | PCT

(10) International Publication Number
WO 2023/287435 A1

(51) International Patent Classification:
G06F 21/62 (2013.01) *G06Q 20/38* (2012.01)

(21) International Application Number:
PCT/US2021/042066

(22) International Filing Date:
16 July 2021 (16.07.2021)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.** [US/US]; 10300 Energy Drive, Spring, Texas 77389 (US).

(72) Inventors: **LUKASIK, Derek**; 3390 E. Harmony Rd., Fort Collins, Colorado 80528 (US). **BALINSKY, Helen**; 1 Redcliff Street, London Bristol BS1 6NP (GB).

(74) Agent: **ANDERSON, Maria C.** et al.; Knobbe, Martens, Olson & Bear, LLC, 2040 Main Street, 14th Floor, Irvine, CA 92614 (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, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, 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 the identity of the inventor (Rule 4.17(i))*

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

(54) Title: BLOCKCHAIN FOR DIGITAL CERTIFICATE TRANSACTIONS

(57) Abstract: In one example in accordance with the present disclosure, an electronic device is described. An example electronic device includes a processor. The example processor is to record information for a digital certificate to a blockchain ledger. The example processor is to authorize a transaction for the digital certificate based on the blockchain ledger.

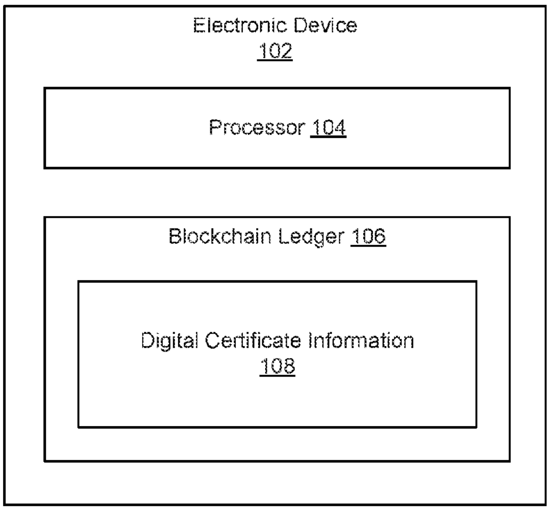

Fig. 1

BLOCKCHAIN FOR DIGITAL CERTIFICATE TRANSACTIONS

BACKGROUND

[0001] Electronic devices may communicate with each other. In some examples, electronic devices may communicate with each other over a network. Some examples of networks include a local area network, a wide area network and the internet. In some examples, network communication may be secured using cryptographic techniques. One example of a cryptographic technique is key authentication using public and private key pairs.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] The accompanying drawings illustrate various examples of the principles described herein and are part of the specification. The illustrated examples are given merely for illustration, and do not limit the scope of the claims.

[0003] Fig. 1 is a block diagram of an electronic device to manage digital certificate transactions, according to an example.

[0004] Fig. 2 is an example of entities to perform digital certificate transactions, according to an example.

[0005] Fig. 3 is a sequence diagram illustrating a process of issuing a digital certificate, according to an example.

[0006] Fig. 4 illustrates transactions for a process of issuing a digital certificate, according to an example.

[0007] Fig. 5 illustrates transactions for a process of issuing a digital certificate, according to another example.

[0008] Fig. 6 depicts a non-transitory machine-readable storage medium for managing digital certificate transactions, according to an example.

[0009] Throughout the drawings, identical reference numbers designate similar, but not necessarily identical, elements. The figures are not necessarily to scale, and the size of some parts may be exaggerated to more clearly illustrate the example shown. Moreover, the drawings provide examples and/or implementations consistent with the description; however, the description is not limited to the examples and/or implementations provided in the drawings.

DETAILED DESCRIPTION

[0010] Digital certificates may be used to establish the identity of web services on a network (e.g., the internet). As used herein, a digital certificate (also referred to as a public key certificate or identity certificate) is an electronic file used to prove ownership of a public key. Trust in the process of issuing and maintaining digital certificates is expected by businesses and individuals to continue using web services. With that basic trust, users may be confident that malicious individuals cannot intercept or otherwise interfere with interactions over an otherwise untrusted network infrastructure (e.g., the internet).

[0011] In some examples, digital certificates that identify web services on the internet are issued by a certificate authority (CA). The process of issuing a digital certificate involves the generation of a public/private key pair by an entity desiring a certificate. This entity may be referred to as the “subject” of the digital certificate. An entity does this by generating a certificate signing request (CSR) including relevant details (e.g., subject, organization, owner, etc.) and then signing the CSR with the corresponding private key. The CSR, along with the public key, is sent to the CA for approval.

[0012] In some examples, the process used by a CA to approve a digital certificate is dependent upon the level of validation used. Three types of validation are: domain validation (DV), organization validation (OV), and extended validation (EV). In DV, the CA challenges the requestor of the digital certificate to prove their control over a domain identified by the subject (or alternate name(s)) of the CSR. With OV, in addition to DV, the validation involves a CA verifying that the organization in the CSR is a valid legal entity. EV is an extension of OV where the CA additionally verifies that the entity requesting the digital certificate is a part of the claimed legal entity. In some examples, EV may include a human performing the verification. Upon receiving a digital certificate, an administrator may include the issued digital certificate within the runtime configuration of the appropriate web service.

[0013] As mentioned, a CA may validate that a requesting entity owns the domain identified by a certificate. In some examples, the CA may perform a challenge-response process starting with the CA issuing a challenge and the requesting entity proving ownership by providing the appropriate response. In some examples, the challenge-response may be a Hypertext Transfer Protocol (HTTP)-based process. In this case, the response is placed within a certain HTTP path for the domain. The CA then performs an HTTP query for the response and accepts or rejects the request.

[0014] In some examples, the challenge-response may be a Domain Name System (DNS)-based process. In this case, the CA may issue a challenge and the requesting entity may prove ownership by placing the appropriate response in a DNS text (TXT) record. The CA then queries for the TXT record via DNS and accepts or rejects the request based on the response.

[0015] The present specification describes examples of automated digital certificate management based on a blockchain ledger. In some examples, a blockchain ledger may be used to cryptographically sign transactions. Each transaction may be cryptographically signed with a hash of the preceding transaction. A new record of a transaction may be added to the blockchain ledger.

[0016] The present specification describes using a smart contract and blockchain ledger for digital certificate management. When managing digital certificate information, a single blockchain ledger may be used as a part of a smart contract. As used herein, a “smart contract” may include instructions stored on an electronic device that automatically execute based on conditions being met. In the examples described herein, the process of managing the lifetime of a digital certificate may be fully automated. These processes may include issuance, revocation and rotation of a digital certificate.

[0017] In some examples, a set of roles and a set of transactions may be defined. For example, entities may be assigned roles and issue transactions to the blockchain ledger. Entities can be individuals, web services or electronic devices (e.g., computers, servers, etc.). Entities may be identified using a public/private keypair with the public key being registered in the blockchain ledger. The smart contract may implement a set of rules (also referred to as logic, or business logic) within a domain. For example, an entity with a domain owner role may be permitted to assign a host device (also referred to as a machine) to a domain. An entity with the host device role may not be permitted to issue certificates.

[0018] In an example, the present specification describes an electronic device. The electronic device includes a processor. In this example, the processor is to record information for a digital certificate to a blockchain ledger. In this example, the processor is to authorize a transaction for the digital certificate based on the blockchain ledger.

[0019] In another example, the present specification also describes an electronic device. The electronic device includes a processor. In this example, the processor is to receive a request from a domain owner entity to initiate a challenge for a digital certificate. The processor is to verify that the domain owner entity is permitted to request the challenge based on a blockchain ledger. The processor is to perform the challenge with a host device and a certificate authority based on the blockchain ledger. The processor is to save the digital certificate to the blockchain ledger in response to a successful challenge. The processor is to send the digital certificate saved in the blockchain ledger to the host device.

[0020] In yet another example, the present specification also describes a non-transitory machine-readable storage medium that includes instructions, when executed by a processor of an electronic device, cause the processor to assign a set of roles for entities performing digital certificate transactions. The instructions also cause the processor to record the set of roles and entity information in a blockchain ledger. The instructions further cause the processor to authorize the digital certificate transactions based on the assigned set of roles and the entity information recorded in the blockchain ledger. The instructions additionally cause the processor to record the digital certificate transactions in the blockchain ledger.

[0021] As used in the present specification and in the appended claims, the term “processor” may be a controller, an application-specific integrated circuit (ASIC), a semiconductor-based microprocessor, a central processing unit (CPU), and a field-programmable gate array (FPGA), and/or other hardware device.

[0022] As used in the present specification and in the appended claims, the term “memory” may include a computer-readable storage medium, which computer-readable storage medium may contain, or store computer-usable program code for use by or in connection with an instruction execution system, apparatus, or device. The memory may take many types of memory including volatile and non-volatile memory. For example, the memory may include Random Access Memory (RAM), Read Only Memory (ROM), optical memory disks, and magnetic disks, among others. The executable code may, when executed by the respective component, cause the component to implement the functionality described herein.

[0023] Turning now to the figures, Fig. 1 is a block diagram of an electronic device 102 to manage digital certificate transactions, according to an example. As described above, the electronic device 102 includes a processor 104. The processor 104 of the electronic device 102 may be implemented as dedicated hardware circuitry or a virtualized logical processor. The dedicated hardware circuitry may be implemented as a central processing unit (CPU). A dedicated hardware CPU may be implemented as a single to many-core general purpose processor. A dedicated hardware CPU may also be implemented as a multi-chip solution, where more than one CPU are linked through a bus and schedule processing tasks across the more than one CPU.

[0024] A virtualized logical processor may be implemented across a distributed computing environment. A virtualized logical processor may not have a dedicated piece of hardware supporting it. Instead, the virtualized logical processor may have a pool of resources supporting the task for which it was provisioned. In this implementation, the virtualized logical processor may be executed on hardware circuitry; however, the hardware circuitry is not dedicated. The hardware circuitry may be in a shared environment where utilization is time sliced. Virtual machines (VMs) may be implementations of virtualized logical processors.

[0025] In some examples, a memory may be implemented in the electronic device 102. The memory may be dedicated hardware circuitry to host instructions for the processor 104 to execute. In another implementation, the memory 104 may be virtualized logical memory. Analogous to the processor 104, dedicated hardware circuitry may be implemented with dynamic random-access memory (DRAM) or other hardware implementations for storing processor instructions. Additionally, the virtualized logical memory may be implemented in an abstraction layer which allows the instructions to be executed on a virtualized logical processor, independent of any dedicated hardware implementation.

[0026] The electronic device 102 may also include instructions. The instructions may be implemented in a platform specific language that the processor 104 may decode and execute. The instructions may be stored in the memory during execution. The instructions may include operations executable by the processor 104 to manage digital certificate transactions. The instructions when executed may enable the processor 104 to record information 108 for a digital certificate to a blockchain ledger 106 and authorize a transaction for the digital certificate based on the blockchain ledger 106.

[0027] In some examples, the processor 104 may implement a smart contract to manage digital certificate transactions. In some examples, the blockchain smart contract for managing digital certificates may include the following roles: host device, domain owner, and certificate authority. The processor 104 may assign a set of roles to different entities involved with the digital certificate. For example, the processor 104 may assign a domain owner entity to a domain owner role. The processor 104 may assign a host device to a host device role. The processor 104 may assign a certificate authority to a certificate authority role.

[0028] The processor 104 may record information 108 for a digital certificate to a blockchain ledger 106. As used herein, a “blockchain ledger” is a series of records (also referred to as blocks) that are linked together using cryptography. Each record in the blockchain ledger 106 may be signed with a cryptographic hash of the previous record. The data in any given record of the blockchain ledger 106 cannot be altered retroactively without altering all subsequent records. As used herein, recording a record to the blockchain ledger 106 may include generating a new record, saving information in the new record and signing the new record with the cryptographic hash of the previous record.

[0029] In some examples, the electronic device 102 that performs the digital certificate management described herein may also host the blockchain ledger 106. For example, the electronic device 102 may store the blockchain ledger 106 in memory. It should be noted that in some examples, the blockchain ledger 106 may be stored in a remote memory location. For example, the electronic device 102 may access the blockchain ledger 106 over a network connection.

[0030] In some examples, the processor 104 may record the set of roles to the blockchain ledger 106. For example, the information recorded to the blockchain ledger 106 may include entity information about the entities assigned to the set of roles for the digital certificate transactions. The processor 104 may record domain owner information, certificate authority information, and/or host device information to the blockchain ledger 106. The domain owner information, certificate authority information, host device information may include information used to identify a domain owner entity, certificate authority and host device, respectively.

[0031] In some examples, the processor 104 may store a public key for each entity within the set of roles in the blockchain ledger 106. For instance, the processor 104 may use a public key to identify an entity. The processor 104 may record the public key of a given entity to the blockchain ledger 106. For example, the domain owner information may include a public key for the domain owner entity. The certificate authority information may include a public key of the certificate authority. The host device information may include a public key of the host device.

[0032] In some examples, the processor 104 may allow a given entity to perform digital certificate transactions based on an assigned role of the entity. For example, the smart contract may allow the domain owner entity to perform a first set of transactions, the host device may perform a second set of transactions and the certificate authority may perform a third set of transactions. As used herein, a “transaction” is an operation performed in the process of issuing, revoking and/or rotating a digital certificate.

[0033] In some examples, a transaction may include identifying a device (e.g., the host device). In some examples, a transaction may include assigning a domain for the digital certificate and assigning a host device to receive the digital certificate. Some examples of transactions may include beginning a challenge for a digital certificate and storing a domain proof in response to the challenge. Examples of transactions may also include issuing the digital certificate, revoking the digital certificate and/or renewing the digital certificate.

[0034] In some examples, the processor 104 may use the public keys stored in the blockchain ledger 106 to validate a transaction for the set of roles. For example, the processor 104 may receive a request for a transaction from an entity. The request may be signed by a private key of the entity. The processor 104 may query the blockchain ledger 106 to obtain the public key for the entity to validate the authenticity of the request.

[0035] In some examples, upon receiving a request for a transaction from an entity, the processor 104 may determine a role of the entity in the blockchain ledger 106. For example, the processor 104 may determine whether the entity is assigned a domain owner role, host device role or certificate authority role. The processor 104 may authorize the request in response to determining that the role of the entity is permitted to perform the transaction. In some examples, a successful transaction may be recorded in the blockchain ledger 106. A failed transaction may result in an error response being sent to the entity requesting the transaction.

[0036] In some examples, once a blockchain ledger 106 with digital certificate transactions has been established, the blockchain ledger 106 may serve as an authoritative, tamper-proof source of truth for domains and the associated digital certificates and servers being used.

[0037] In some examples, the processes associated with managing digital certificates may be automated. Furthermore, the verification process may be extended to include automation for OV and EV digital certificates. For example, automated mechanisms may be used to establish corporate identities (e.g., via governmental records) and/or individual identities within those corporations (e.g., via LDAP).

[0038] The blockchain-based certificate management described herein may explicitly record and enforce the roles of each entity involved in issuing a digital certificate. The blockchain-based certificate management described may also incorporate a digital certificate revocation process.

[0039] Fig. 2 is an example of entities that may perform digital certificate transactions, according to an example. In this example, a domain owner entity 212, a host device 214 and a certificate authority 216 may be assigned a role in a set of roles 218. For example, as described above, the domain owner entity 212 may be assigned 201a a domain owner role, the host device 214 may be assigned 201b a host device role, and the certificate authority 216 may be assigned 201c a certificate authority role.

[0040] In some examples, the smart contract 220 may be implemented by the processor 102 described in Fig. 1. The smart contract 220 may record the set of roles 218 in the blockchain ledger 106.

[0041] The domain owner entity 212, host device 214 and/or certificate authority 216 may create 203a-c a request for a transaction 210. Some examples of the types of transactions 210 that may be received at the smart contract 220 include device identity, a challenge issued by the certificate authority 216, a proof (e.g., DNS proof, HTTP proof) provided by the host device 214, issuing the digital certificate, and/or revoking the digital certificate.

[0042] The smart contract 220 may receive the transaction request, which triggers 205 the smart contract 220 to verify 207 that the entity requesting the transaction 210 belongs to the set of roles 218 recorded in the blockchain ledger 106. If the smart contract 220 determines that the requesting entity is permitted to request the transaction 210, the smart contract 220 may record 211 the transaction 210 to the blockchain ledger 106. In the case that the requesting entity is a domain owner entity 212 or a host device 214, the smart contract 220 may verify 209 that the requesting entity belongs to the domain 224 associated with the digital certificate. The certificate authority 216 may issue 213 the digital certificate 222 based on the verification of the transaction 210 by the smart contract 220.

[0043] Fig. 3 is a sequence diagram illustrating a process of issuing a digital certificate, according to an example. In one example, the domain owner entity 212, host device 214 and certificate authority 216 may be implemented as the examples described in reference to Fig. 2. In some examples, a blockchain service 326 may be hosted on an electronic device 102 as described in reference to Fig. 1. For example, the operations implemented by the blockchain service 326 may be performed by the processor 104 of the electronic device 102. In some examples, the blockchain service 326 may implement a smart contract 220 as described in reference to Fig. 2.

[0044] At 301, the blockchain service 326 may assign a domain owner role to the domain owner entity 212. The blockchain service 326 may record a public key of the domain owner entity 212 and the domain owner role to the blockchain ledger.

[0045] At 303, the blockchain service 326 may assign a host device role to the host device 214 of a domain. The blockchain service 326 may record a public key of the host device 214 and the host device role to the blockchain ledger.

[0046] At 305, the blockchain service 326 may assign a certificate authority role to the certificate authority 216. The blockchain service 326 may record a public key of the certificate authority 216 and the certificate authority role to the blockchain ledger.

[0047] The public key for each entity with an assigned role is stored in the ledger and may be used by the blockchain service 326 to validate subsequent requests for that role. For example, the blockchain service 326 may store public keys of the domain owner entity 212, the certificate authority 216, and the host device 214 in the blockchain ledger. The blockchain service 326 may validate communications from the domain owner entity, the certificate authority, and the host device based on the public keys stored in the blockchain ledger.

[0048] At 307, the domain owner entity 212 may assign the host device 214 to the domain. In some examples, the smart contract of the blockchain service 326 may ensure that the domain owner entity 212 submitting the request is in the domain owner role. The request is rejected if the request is not signed by the domain owner entity 212. The transaction to assign the host device 214 may be stored in the blockchain ledger.

[0049] At 309, the domain owner entity 212 may start a challenge to receive a digital certificate for the domain. In some examples, the challenge may be an HTTP challenge or a DNS challenge. The blockchain service 326 may receive the request from the domain owner entity 212 to initiate the challenge for a digital certificate. The blockchain service 326 may verify that the domain owner entity 212 is permitted to request the challenge based on the blockchain ledger. For example, the blockchain service 326 may determine that the domain owner entity 212 is assigned to the domain owner role in the blockchain ledger. The blockchain service 326 may reject the transaction if the request is not signed by the domain owner entity 212 recorded in the blockchain ledger.

[0050] The blockchain service 326 may perform the challenge with the host device 214 and the certificate authority 216 based on the blockchain ledger. For example, at 311, the certificate authority 216 may create a challenge value in response to the challenge request. The blockchain service 326 may record the challenge value received from the certificate authority in the blockchain ledger. At 313, the host device 214 hosting the domain may query the blockchain ledger for the challenge value. The blockchain service 326 may validate that the signature of the host device 214 matches the domain assignment from 307. The blockchain service 326 may send the challenge value to the host device 214 in response to a request (i.e., the query) for the challenge value received from the host device 214.

[0051] At 315, the host device 214 may solve the challenge. In the case of HTTP, the host device 214 may present the challenge response via an HTTP endpoint. At 317, the blockchain service 326 may receive a notification that the host device 214 solved the challenge. The blockchain service 326 may then notify the certificate authority 216 that the host device 214 has solved the challenge.

[0052] At 319, the certificate authority 216 may validate the challenge response. For example, the certificate authority 216 may perform an HTTP GET query for the challenge response. The certificate authority 216 may then validate the result of the challenge response. Upon validating the challenge response, the certificate authority 216 may retrieve relevant metadata for the host device 214, the domain and the digital certificate. The certificate authority 216 may sign and send a digital certificate in a blockchain transaction, at 321.

[0053] Upon receiving the digital certificate from the certificate authority 216, the blockchain service 326 may validate the transaction signature as being from an entity within the certificate authority role. The blockchain service 326 may then record the transaction for the certificate authority 216 issuing the digital certificate in the blockchain ledger.

[0054] At 323, the host device 214 may query the blockchain service 326 for the digital certificate. The blockchain service 326 may validate that the query is signed by the entity matching the host device role. The blockchain service 326 may then send the digital certificate saved in the blockchain ledger to the host device 214 in response to the request received from the host device 214 for the digital certificate.

[0055] Fig. 4 illustrates transactions 401 for a process of issuing a digital certificate, according to an example. In one example, the domain owner entity 212, host device 214 and certificate authority 216 may be implemented as the examples described in reference to Fig. 2. The blockchain service 326 of Fig. 3 may be hosted on an electronic device 102 as described in reference to Fig. 1. In some examples, the blockchain service 326 of Fig. 3 may record transactions 401 to a blockchain ledger 106.

[0056] At 403, the domain owner entity 212 may trigger a process assigning the host device 214 to a domain address. A transaction (T1) 401-1 for assigning the host device 214 may be recorded in the blockchain ledger 106. At 405, the host device 214 may be notified of the assignment.

[0057] At 407, the host device 214 may present a digital certificate request for the assigned domain. A transaction (T2) 401-2 for the digital certificate request may be recorded in the blockchain ledger 106.

[0058] At 409, the certificate authority 216 may be notified of the digital certificate request. In response to the digital certificate request, the certificate authority 216 may generate a challenge value, at 411. A transaction (T3) 401-3 for the challenge value may be recorded in the blockchain ledger 106. At 413, the host device 214 may be notified of the challenge from the certificate authority 216.

[0059] At 415, the host device 214 may query the challenge value stored in transaction (T3) 401-3 of the blockchain ledger. At 417, upon receiving the challenge value, the host device 214 may present a challenge response at an expected universal resource locator (URL). A transaction (T4) 401-4 for the challenge response may be recorded in the blockchain ledger 106.

[0060] At 419, certificate authority 216 may be notified of the challenge response. At 421, the certificate authority 216 may verify the challenge response by querying URL. In some examples, the certificate authority 216 may cache the challenge value. In some examples, the certificate authority 216 may be stateless and may read the challenge value from transaction (T3) 401-3 of the blockchain ledger 106 for verification.

[0061] At 423, the certificate authority 216 may issue a digital certificate as a blockchain transaction 401-5. The certificate authority 216 may submit the transaction (T5) 401-5 to the blockchain ledger 106.

[0062] At 425, the host device 214 may be notified of the digital certificate issuance. At 427, the host device 214 may query (e.g., receive) the digital certificate from the blockchain ledger 106. In some examples, other parties may also query the digital certificate of the host device 214 from the blockchain ledger 106.

[0063] It should be noted that the example of Fig. 4 uses HTTP in the proof to the challenge. In some examples, a DNS proof path with blockchain may be used. In this approach, the host device 214 hosting the web service may be removed from the proof process. Instead, a DNS server entry may be used to establish proof to the challenge.

[0064] Fig. 5 illustrates transactions 501 for a process of issuing a digital certificate, according to another example. In one example, the domain owner entity 212 and host device 214 may be implemented as the examples described in reference to Fig. 2. The blockchain service 326 of Fig. 3 may be hosted on an electronic device 102 as described in reference to Fig. 1. In some examples, the blockchain service 326 of Fig. 3 may record transactions 401 to a blockchain ledger 106.

[0065] The example of Fig. 5 may be used for organization validation and/or extended validation. At 503, a domain owner entity 212 may purchase the host device 214 from a machine vendor 528. At the time of sale, the machine vendor 528 may verify, at 505, the legal entity 530 (e.g., the entity and organization) ordering the host device 214. At 507, the machine vendor 528 may record the purchase information in a blockchain transaction (T1) 501-1.

[0066] The transaction (T1) 501-1 recorded in the blockchain ledger 106 may be used for organization validation and/or extended validation with issued digital certificates. For example, the host device 214 may request a digital certificate for a domain from the machine vendor 528. In this example, the machine vendor 528 may act as a certificate authority. If domain validation is successful, the digital certificate may include metadata identifying the organization that owns and/or operates the host device 214.

[0067] At 509, the host device 214 may establish its identity in the blockchain ledger 106. This may be accomplished as described in Fig. 3. A transaction (T2) 501-2 for provisioning the host device identity may be recorded in the blockchain ledger 106. At 511, the domain owner entity 212 may trigger a process assigning the host device 214 to a domain address. A transaction (T3) 501-3 for assigning the host device 214 may be recorded in the blockchain ledger 106. At 513, the process to issue a digital certificate may proceed as described in Fig. 4, where the machine vendor 528 operates as the certificate authority 216.

[0068] At 515, the machine vendor 528 may include OV/EV information in the issued digital certificate using the information from the ledger established in transaction (T1) 501-1. At 517, the machine vendor 528 record the issued digital certificate in transaction (T4) 501-4 to the blockchain ledger 106.

[0069] Fig. 6 depicts a non-transitory machine-readable storage medium 632 for managing digital certificate transactions, according to an example. To achieve its desired functionality, an electronic device 102 includes various hardware components. Specifically, an electronic device 102 includes a processor and a machine-readable storage medium 632. The machine-readable storage medium 632 is communicatively coupled to the processor. The machine-readable storage medium 632 includes a number of instructions 634, 636, 638, 640 for performing a designated function. The machine-readable storage medium 632 causes the processor to execute the designated function of the instructions 634, 636, 638, 640. The machine-readable storage medium 632 can store data, programs, instructions, or any other machine-readable data that can be utilized to operate the electronic device 102. Machine-readable storage medium 632 can store computer readable instructions that the processor of the electronic device 102 can process, or execute. The machine-readable storage medium 632 can be an electronic, magnetic, optical, or other physical storage device that contains or stores executable instructions. Machine-readable storage medium 632 may be, for example, Random Access Memory (RAM), an Electrically Erasable Programmable Read-Only Memory (EEPROM), a storage device, an optical disc, etc. The machine-readable storage medium 632 may be a non-transitory machine-readable storage medium 632, where the term “non-transitory” does not encompass transitory propagating signals.

[0070] Referring to Fig. 6, role assignment instructions 634, when executed by the processor, cause the processor to assign a set of roles for entities performing digital certificate transactions. Role and entity record instructions 636, when executed by the processor, may cause the processor to record the set of roles and entity information in a blockchain ledger. Transaction authorization instructions 638, when executed by the processor, may cause the processor to authorize the digital certificate transactions based on the assigned set of roles and the entity information recorded in the blockchain ledger. In some examples, the digital certificate transactions may include transactions for domain validation, organization validation, or an extended validation. Transaction record instructions 640, when executed by the processor, may cause the processor to record the digital certificate transactions in the blockchain ledger.

[0071] In some examples, the instructions, when executed by the processor, cause the processor to identify an entity using a public key of the entity recorded in the blockchain ledger. For example, upon receiving a request for a digital certificate transaction from an entity, the processor may retrieve the public key for the entity from the blockchain ledger. The processor may then use the public key to verify that the request is signed by the entity.

[0072] In some examples, the instructions, when executed by the processor, cause the processor to authorize a given digital certificate transaction based on a record of an earlier digital certificate transaction recorded in the blockchain ledger. For example, the processor may determine that a request for a digital certificate transaction is signed with a private key corresponding to the public key recorded in the blockchain ledger.

[0073] In some examples, the instructions, when executed by the processor, cause the processor to receive a request to perform a given digital certificate transaction from an entity. The processor may determine a role of the entity based on the set of roles and entity information recorded in the blockchain ledger. The processor may authorize the entity to perform the given digital certificate transaction based on the role of the entity. The processor may record the given digital certificate transaction in the blockchain ledger.

CLAIMS

What is claimed is:

1. An electronic device, comprising:

a processor to:

record information for a digital certificate to a blockchain ledger; and

authorize a transaction for the digital certificate based on the blockchain ledger.

2. The electronic device of claim 1, wherein the information recorded to the blockchain ledger comprises domain owner information, certificate authority information, and host device information for a device that is to receive the digital certificate.

3. The electronic device of claim 1, wherein the processor is to:

assign a set of roles comprising a domain owner role, a certificate authority role and a host device role to different entities; and

record the set of roles to the blockchain ledger.

4. The electronic device of claim 3, wherein the processor is to:

store a public key for each entity within the set of roles in the blockchain ledger; and

use the stored public keys to validate a transaction for the set of roles.

5. The electronic device of claim 1, wherein the processor is to:

receive a request for a transaction from an entity;

determine a role of the entity in the blockchain ledger; and

authorize the request in response to determining that the role of the entity is permitted to perform the transaction.

6. An electronic device, comprising:

a processor to:

receive a request from a domain owner entity to initiate a challenge for a digital certificate;

verify that the domain owner entity is permitted to request the challenge based on a blockchain ledger;

perform the challenge with a host device and a certificate authority based on the blockchain ledger;

save the digital certificate to the blockchain ledger in response to a successful challenge; and

send the digital certificate saved in the blockchain ledger to the host device.

7. The electronic device of claim 6, wherein the processor is to verify that the domain owner entity is permitted to request the challenge based on a public key of the domain owner entity stored in the blockchain ledger.

8. The electronic device of claim 6, wherein the processor to perform the challenge with a host device and a certificate authority comprises the processor to:

record a challenge value received from the certificate authority in the blockchain ledger;

send the challenge value to the host device in response to a request for the challenge value received from the host device;

receive a notification that the host device solved the challenge;

notify the certificate authority that the host device has solved the challenge; and

receive the digital certificate from the certificate authority.

9. The electronic device of claim 6, wherein the processor is to:

store public keys of the domain owner entity, the certificate authority, and the host device in the blockchain ledger; and validate communications from the domain owner entity, the certificate authority, and the host device based on the public keys stored in the blockchain ledger.

10. The electronic device of claim 6, wherein the processor is to:
send the digital certificate saved in the blockchain ledger to the host device in response to a request received from the host device for the digital certificate.

11. A non-transitory machine-readable storage medium comprising instructions, when executed by a processor of an electronic device, cause the processor to:
assign a set of roles for entities performing digital certificate transactions;
record the set of roles and entity information in a blockchain ledger;
authorize the digital certificate transactions based on the assigned set of roles and the entity information recorded in the blockchain ledger; and
record the digital certificate transactions in the blockchain ledger.

12. The non-transitory machine-readable storage medium of claim 12, wherein, the digital certificate transactions comprise transactions for domain validation, organization validation, or an extended validation.

13. The non-transitory machine-readable storage medium of claim 12, wherein the instructions, when executed by the processor, cause the processor to identify an entity using a public key of the entity recorded in the blockchain ledger.

14. The non-transitory machine-readable storage medium of claim 12, wherein the instructions, when executed by the processor, cause the processor to authorize a given digital certificate transaction based on a record of an earlier digital certificate transaction recorded in the blockchain ledger.

15. The non-transitory machine-readable storage medium of claim 12, wherein the instructions, when executed by the processor, cause the processor to:

receive a request to perform a given digital certificate transaction from an entity;

determine a role of the entity based on the set of roles and entity information recorded in the blockchain ledger;

authorize the entity to perform the given digital certificate transaction based on the role of the entity; and

record the given digital certificate transaction in the blockchain ledger.

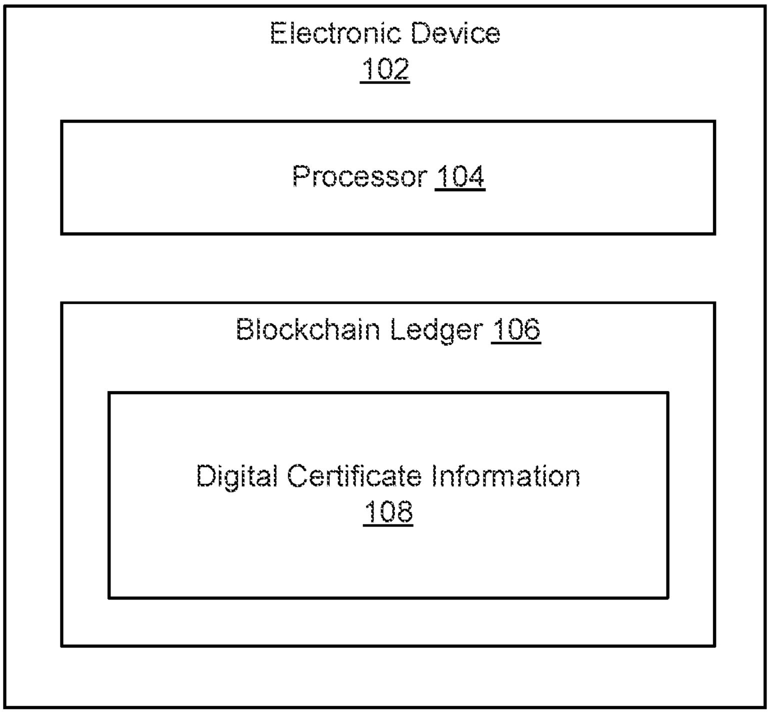
Electronic Device
102
Processor 104
Blockchain Ledger 106
Digital Certificate Information
108

Fig. 1

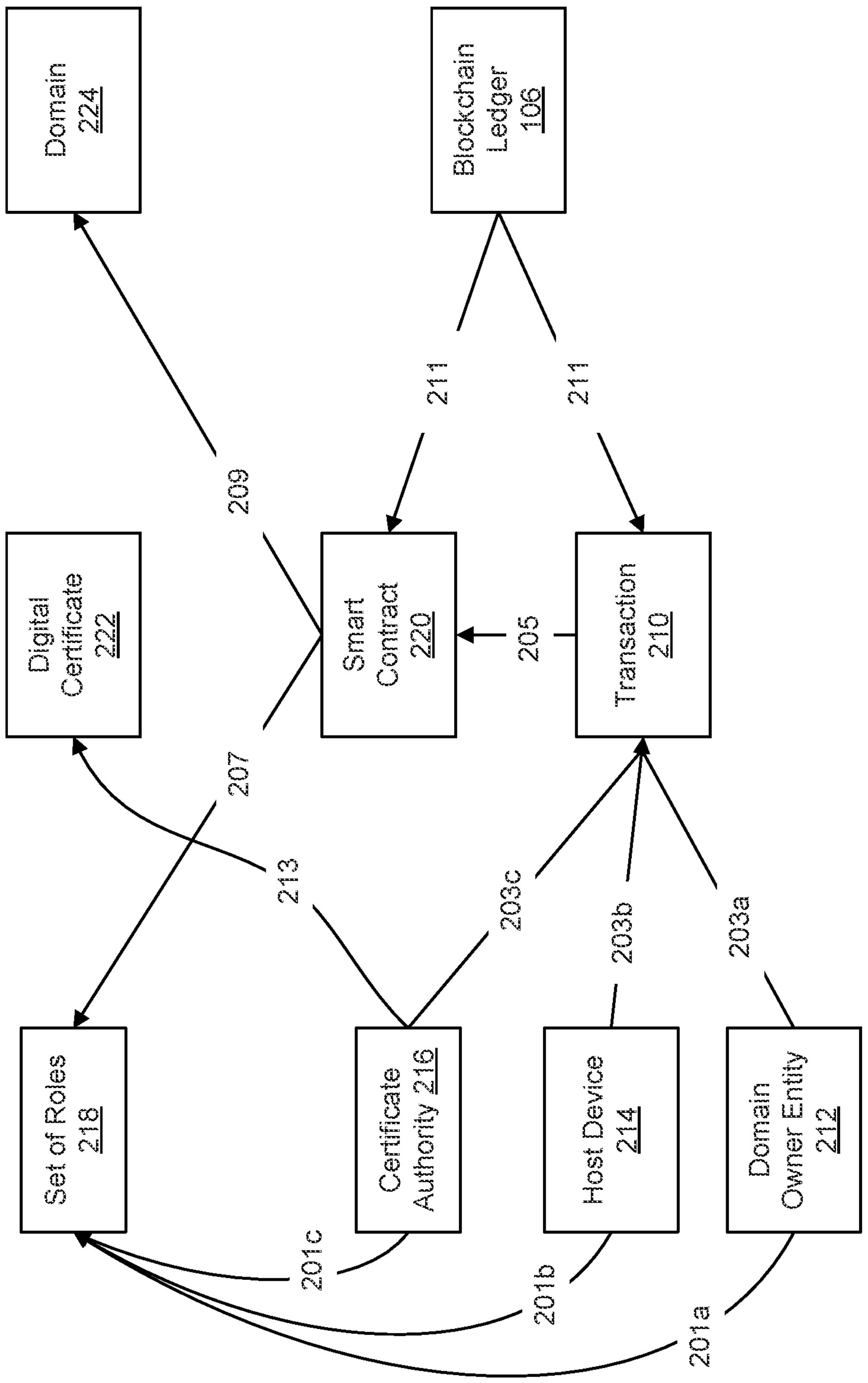
Domain Owner Entity 212
Host Device 214
Certificate Authority 216
Set of Roles 218
201a
201b
201c
203a
203b
203c
Transaction 210
205
Smart Contract 220
207
209
213
Digital Certificate 222
Domain 224
211
211
Blockchain Ledger 106

Fig. 2

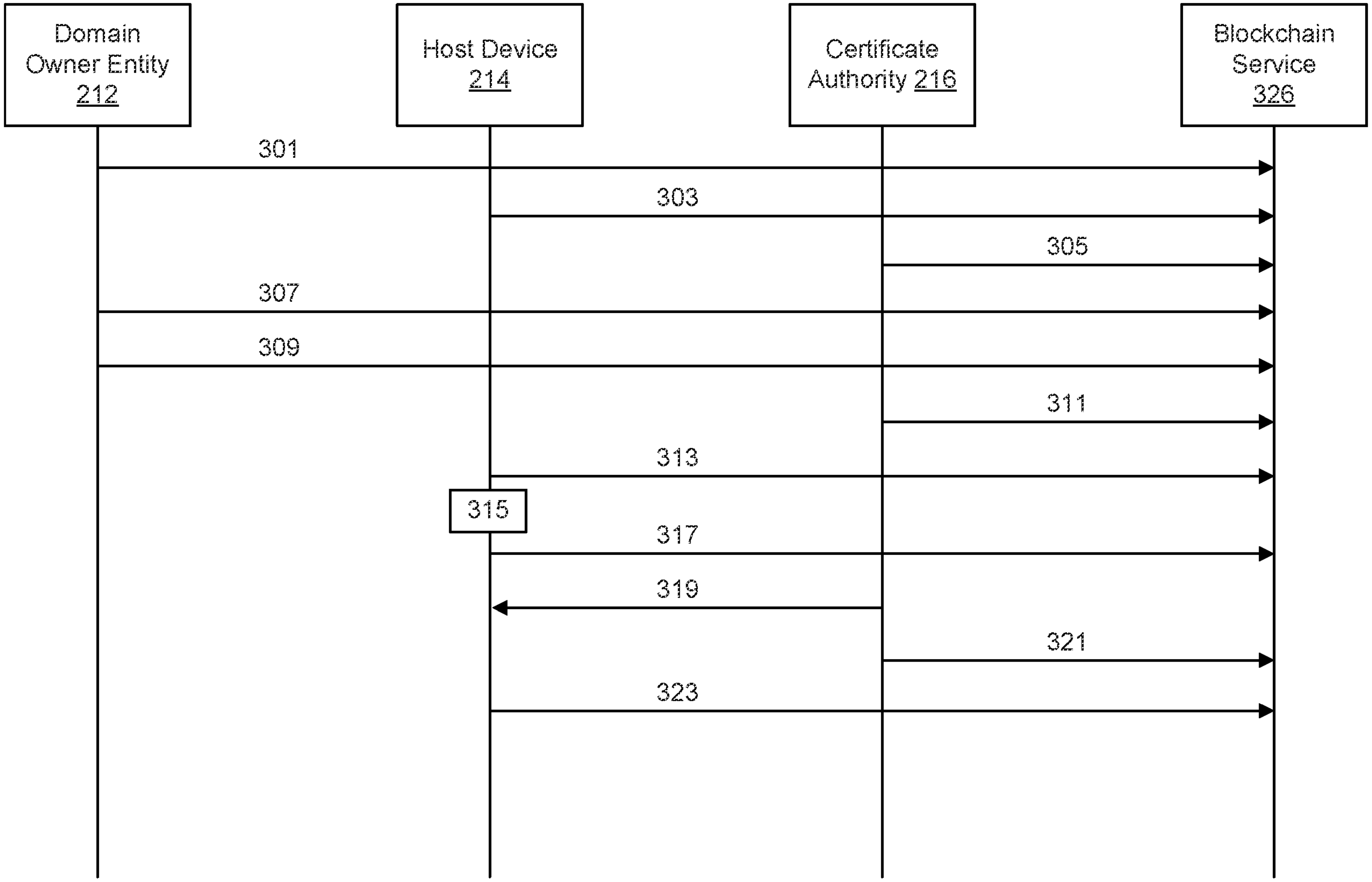
Domain Owner Entity 212
Host Device 214
Certificate Authority 216
Blockchain Service 326
301
303
305
307
309
311
313
315
317
319
321
323

Fig. 3

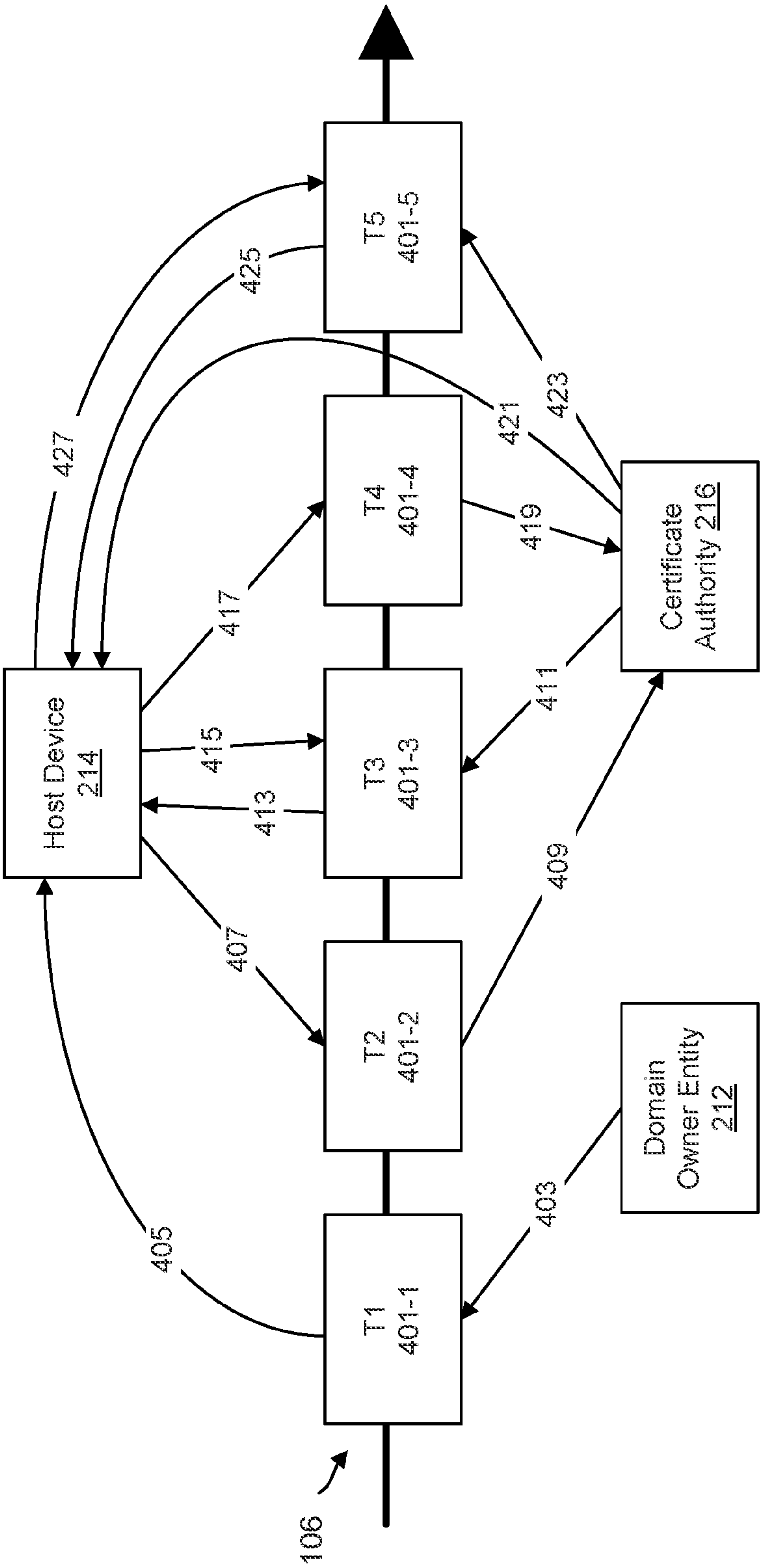
106
T1
401-1
T2
401-2
T3
401-3
T4
401-4
T5
401-5
Host Device
214
Certificate
Authority 216
Domain
Owner Entity
212
403
405
407
409
411
413
415
417
419
421
423
425
427

Fig. 4

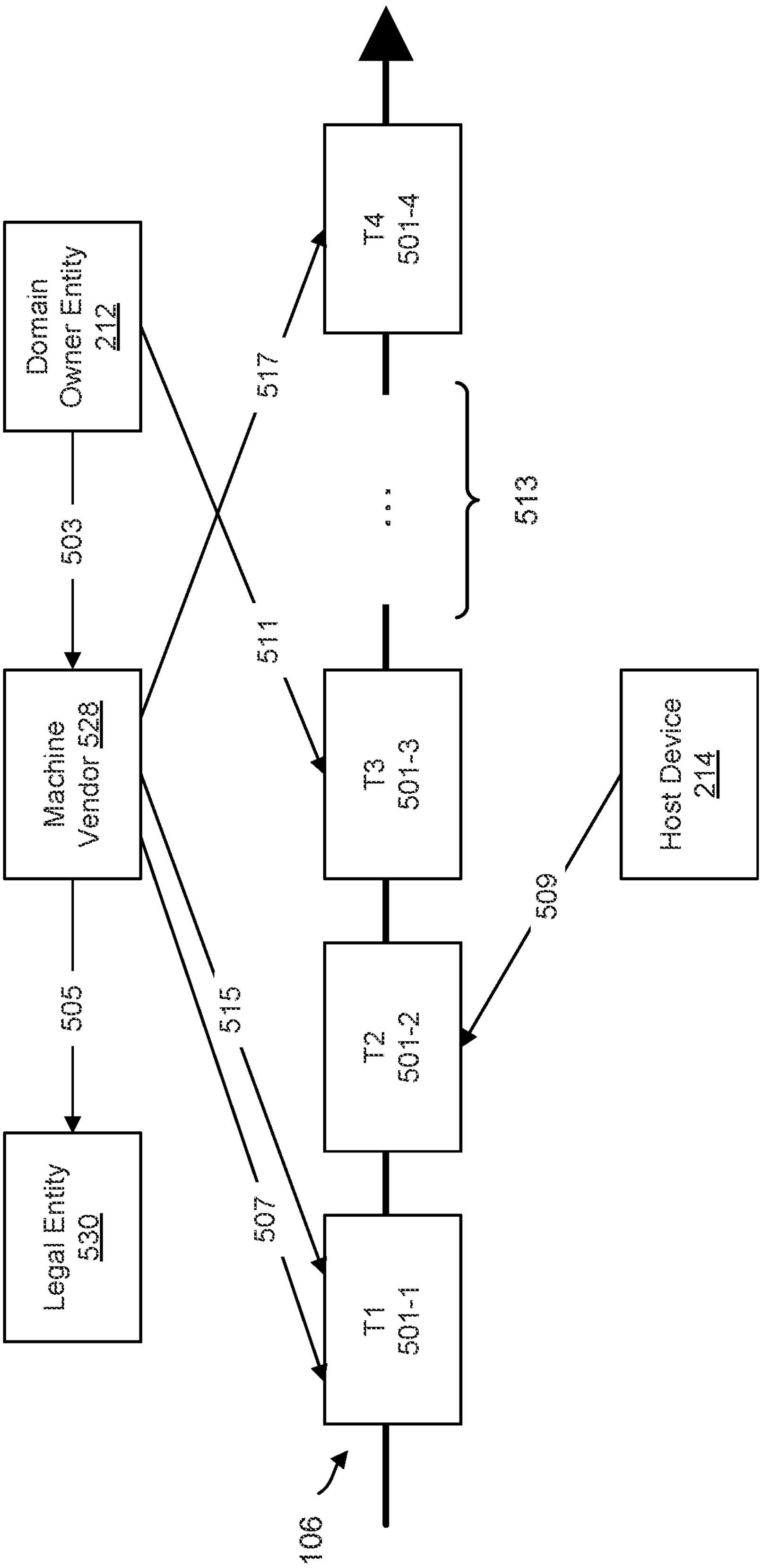
Domain Owner Entity 212
Machine Vendor 528
Legal Entity 530
503
505
507
515
511
517
T1 501-1
T2 501-2
T3 501-3
T4 501-4
. . .
513
509
Host Device 214
106

Fig. 5

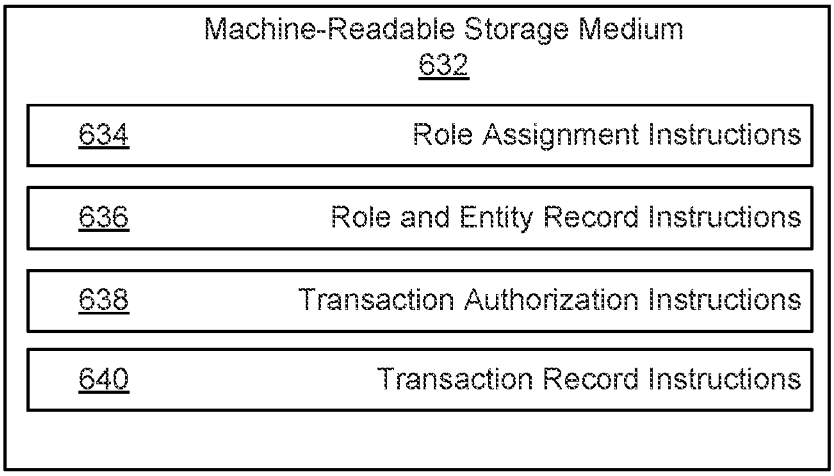
Machine-Readable Storage Medium
632
634 Role Assignment Instructions
636 Role and Entity Record Instructions
638 Transaction Authorization Instructions
640 Transaction Record Instructions

Fig. 6

INTERNATIONAL SEARCH REPORT	International application No. PCT/US 2021/042066

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/62 *(2013.01)*
G06Q 20/38 *(2012.01)*

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 21/00-21/62, G06Q 20/00-20/38

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)

PatSearch (RUPTO internal), USPTO, PAJ, Esp@cenet, Information Retrieval System of FIPS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2020/0021446 A1 (NOKIA TECHNOLOGIES OY) 16.01.2020, abstract, paragraphs [0018], [0094], [0124], [0134], [0192], [0208], [0259]-[0263], claims 34, 39	1-9, 11-15
Y		10
Y	US 2020/0007346 A1 (JONATHAN SEAN CALLAN et al) 02.01.2020, abstract, paragraphs [0028], [0137], [0138]	10
A	US 2020/0035059 A1 (TYCO INTEGRATED SECURITY LLC) 30.01.2020	1-15
A	WO 2020/014399 A1 (LISTAT LTD) 16.01.2020	1-15

□ Further documents are listed in the continuation of Box C. □ See patent family annex.

*	Special categories of cited documents:	"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
"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	"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
"E"	earlier document 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)	"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
"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	"&"	document member of the same patent family

Date of the actual completion of the international search 21 March 2022 (21.03.2022)	Date of mailing of the international search report 07 April 2022 (07.04.2022)
Name and mailing address of the ISA/RU: Federal Institute of Industrial Property, Berezhkovskaya nab., 30-1, Moscow, G-59, GSP-3, Russia, 125993 Facsimile No: (8-495) 531-63-18, (8-499) 243-33-37	Authorized officer V. Shepelev Telephone No. (495) 531-64-81