Innovation, Sciences et Développement économique Canada
Office de la Propriété Intellectuelle du Canada

Innovation, Science and Economic Development Canada
Canadian Intellectual Property Office

CA 3090896 A1 2019/08/15

(21) 3 090 896

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2019/02/12
(87) Date publication PCT/PCT Publication Date: 2019/08/15
(85) Entrée phase nationale/National Entry: 2020/08/11
(86) N° demande PCT/PCT Application No.: CA 2019/050177
(87) N° publication PCT/PCT Publication No.: 2019/153095
(30) Priorité/Priority: 2018/02/12 (US62/629,412)

(51) Cl.Int./Int.Cl. *G06Q 10/00* (2012.01), *G06F 16/27* (2019.01), *G16H 40/20* (2018.01)

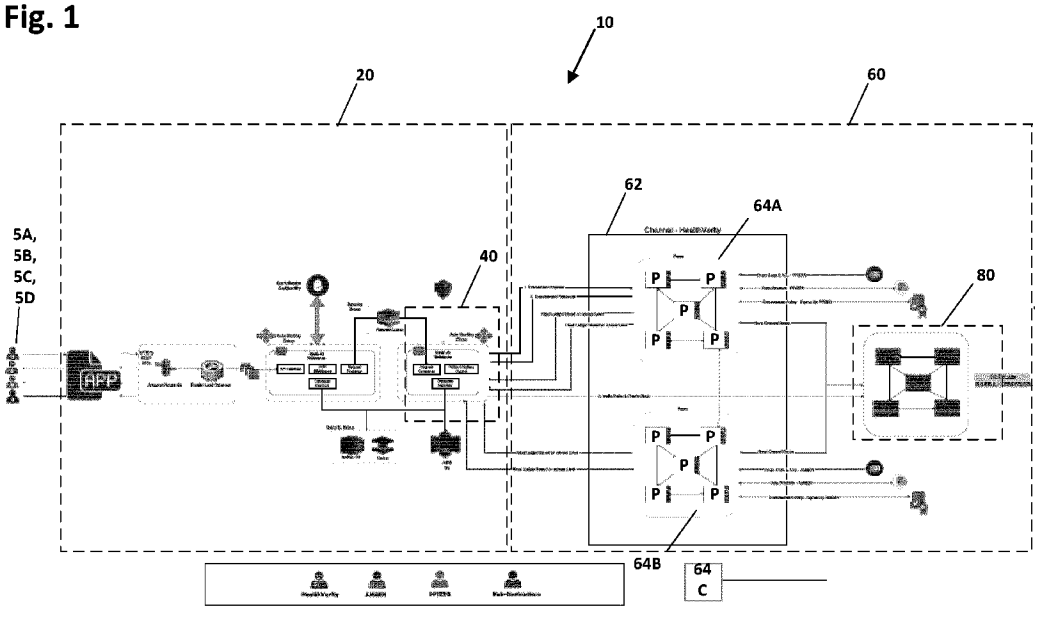
(71) Demandeur/Applicant:
DLT LABS INC., CA

(72) Inventeur/Inventor:
SRIVASTAVA, NEERAJ, CA

(74) Agent: DICKINSON WRIGHT LLP

(54) Titre : SYSTEME ET PROCEDE DE GESTION DE CONSENTEMENT BASE SUR UNE CHAINE DE BLOCS
(54) Title: BLOCKCHAIN-BASED CONSENT MANAGEMENT SYSTEM AND METHOD

Fig. 1



(57) Abrégé/Abstract:
A blockchain-based consent management system includes a webserver subsystem configured to receive and handle authorized web user requests for access to and/or transactions corresponding to consent data for a blockchain, the webserver subsystem comprising a blockchain subsystem interface; and a blockchain subsystem defining a channel having at least two organizations, corresponding chaincode and an endorsement policy, each of the at least two organizations having at least one peer, each of the at least one peer maintaining a blockchain copy, the blockchain subsystem comprising an orderer in communication with the blockchain subsystem interface.

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 August 2019 (15.08.2019)

WIPO | PCT

(10) International Publication Number
WO 2019/153095 A1

(51) International Patent Classification:
G06Q 10/00 (2012.01) *G16H 40/20* (2018.01)
G06F 16/27 (2019.01)

(21) International Application Number:
PCT/CA2019/050177

(22) International Filing Date:
12 February 2019 (12.02.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/629,412 12 February 2018 (12.02.2018) US

(71) Applicant: **DLT LABS INC.** [CA/CA]; 141 Adelaide Street West, Suite 1002, Toronto, Ontario M5H 3L5 (CA).

(72) Inventor: **SRIVASTAVA, Neeraj**; 8 Rean Drive, Gvu218, Toronto, Ontario M2K 3B9 (CA).

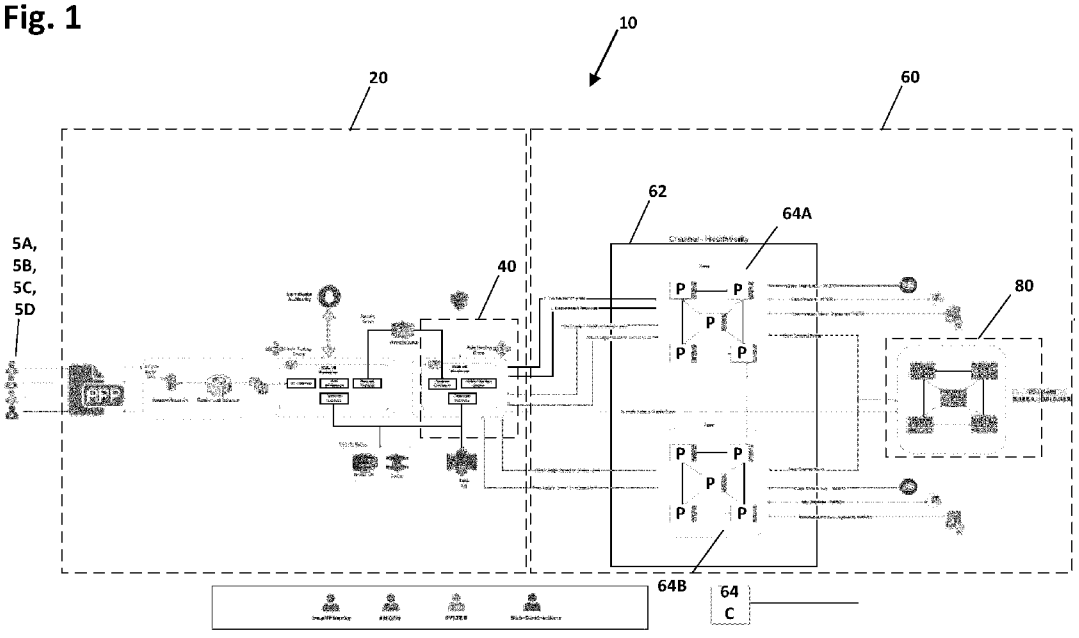
(74) Agent: **GILBERT'S LLP**; 77 King Street West, Suite 2010, Toronto, Ontario M5K 1K2 (CA).

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

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

(54) Title: BLOCKCHAIN-BASED CONSENT MANAGEMENT SYSTEM AND METHOD

Fig. 1



(57) **Abstract:** A blockchain-based consent management system includes a webserver subsystem configured to receive and handle authorized web user requests for access to and/or transactions corresponding to consent data for a blockchain, the webserver subsystem comprising a blockchain subsystem interface; and a blockchain subsystem defining a channel having at least two organizations, corresponding chaincode and an endorsement policy, each of the at least two organizations having at least one peer, each of the at least one peer maintaining a blockchain copy, the blockchain subsystem comprising an orderer in communication with the blockchain subsystem interface.

WO 2019/153095 A1

[Continued on next page]

WO 2019/153095 A1

Declarations under Rule 4.17:

— *as to the identity of the inventor (Rule 4.17(i))*
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

— *with international search report (Art. 21(3))*
— *in black and white; the international application as filed contained color or greyscale and is available for download from PATENTSCOPE*

BLOCKCHAIN-BASED CONSENT MANAGEMENT SYSTEM AND METHOD

Cross Reference to Related Application

[0001] This application claims priority to United States Provisional Patent Application Serial No. 62/629,412 filed on February 12, 2018, the contents of which are incorporated herein by reference in their entirety.

Field of the Invention

[0002] The following relates generally to computer-implemented healthcare and other patient and stakeholder consent management systems, and more particularly to a blockchain-based consent management system and method.

Background of the Invention

[0003] Proper and efficient obtaining, managing, maintaining and sharing of consents for healthcare provision systems is challenging. This is particularly because patients' personal or healthcare related information, including consents, is considered highly sensitive such that it requires careful and secure handling. Furthermore, the number of stakeholders in healthcare systems – patients, regulators, doctors, hospitals, clinics, emergency personnel, pharmaceutical companies conducting clinical trials, regulators, and the like – each having respective methods of collecting and managing consents, is large and varied. Furthermore, there are various types of consents, each having respective considerations. For example, consents can include: consents to treat a patient, consent to protect information for a patient, patient rights, marketing consents, auto-dial consents, customizable consents, informed consents, and consents to share information. Other forms of consents are possible and may be required as healthcare regulations, treatments and systems evolve. Consents may differ across jurisdictions, and may differ depending on the nature or age of the patient and his or her capacity to grant them.

[0004] Various systems have been proposed for centralizing the management of consents for patients and other healthcare system stakeholders. More recently, systems have been proposed that leverage blockchain for immutable and long-term storage of data regarding consents and for controlling access to the immutable consent records for patients. For example, United States Patent Application Publication No. 2018/0082023 to Curbera et al. discloses a secure distributed patient consent and information management system and method for enabling one health provider to directly request patient

information from another health provider using a patient record locator provided by a master patient record index.

[0005] While systems and methods have been proposed, improvements are desirable.

Summary of the Invention

[0006] In accordance with an aspect, there is provided a blockchain-based consent management system comprising a webserver subsystem configured to receive and handle authorized web user requests for access to and/or transactions corresponding to consent data for a blockchain, the webserver subsystem comprising a blockchain subsystem interface; and a blockchain subsystem defining a channel having at least two organizations, corresponding chaincode and an endorsement policy, each of the at least two organizations having at least one peer, each of the at least one peer maintaining a blockchain copy, the blockchain subsystem comprising an orderer in communication with the blockchain subsystem interface.

[0007] In an embodiment, the blockchain subsystem and the webserver subsystem communicate such that authorized requests for transactions for the blockchain cause the webserver subsystem to generate transaction proposals to be routed via the blockchain subsystem interface to the channel peers of the blockchain subsystem for individual endorsement, to receive endorsement responses from the peers, and to, in the event the endorsement responses collectively satisfy the endorsement policy, transmit the endorsed transactions to the orderer for inclusion in an additional block of the blockchain, wherein the orderer is configured to cause the additional block to be stored in each of the peers' blockchain copy.

[0008] In an embodiment, the webserver subsystem is in communication with a certificate authority for the system.

[0009] In an embodiment, the webserver subsystem comprises a first auto-scaling group in communication with a second auto-scaling group via a request queue, wherein the first auto-scaling group lodges requests corresponding to user requests in the request queue for consumption by the second auto-scaling group.

[0010] In an embodiment, the first auto-scaling group comprises one or more Node JS webservers having user interface and application middleware components.

[0011] In an embodiment, the second auto-scaling group comprises one or more Node JS webservers having instances of a hyperledger fabric interface.

[0012] In an embodiment, the webserver subsystem further comprises load balancing components for routing the user requests to webserver instances in the first auto-scaling group.

[0013] Embodiments disclosed herein provide various advantages. For example, a blockchain-based system provides benefits of security, confidentiality and auditability in order to protect consent information. The consent information stored as disclosed herein in a blockchain is immutable and extremely difficult to penetrate without proper authorization, i.e., to hack.

[0014] Embodiments employing the web-based application provide powerful controls over access and additions to blockchain data without imposing a significant limitation on how authorized users can interact with the system and its data, and is suitable for enabling deployment of other application features that may not directly relate to the blockchain data. Embodiments of the system disclosed herein are also easily scaled to incorporate additional entities such as organizations and peers, to deploy new or more sophisticated business logic via new or modified chaincodes, and to adjust and deploy access control lists. The flexibility of the system permits the network to grow, become more sophisticated, to adapt to regulatory and other changes, and generally to become more valuable to its users without undue disruptions as it does.

[0015] Embodiments disclosed herein address potential network traffic bottlenecks by providing auto-scaling groups and/or load balancing and/or use of cloud services to automatically expand and contract the system or to provide better geographic availability in response to increases and decreases in user-bases following from changes made to organizations, additions or removal of organizations, peers and other modifications to the network.

[0016] Various other embodiments and advantages will become apparent from the following description and drawings.

Brief Description of the Drawings

[0017] Embodiments of the invention will now be described with reference to the appended drawings in which:

[0018] Figure 1 is a schematic diagram showing a blockchain-based consent management system, according to an embodiment;

[0019] Figure 2 is an enlarged schematic diagram showing components of a webserver subsystem of the blockchain-based consent management system of Figure 1;

[0020] Figure 3 is an enlarged schematic diagram showing components of a blockchain subsystem of the blockchain-based consent management system of Figure 1; and

[0021] Figure 4 is a schematic diagram showing a hardware architecture of a computing system suitable as a hardware platform for one or more components of the blockchain-based consent management system of Figure 1, according to an embodiment.

Detailed Description

[0022] Figure 1 is a schematic diagram showing a computer-based blockchain-based consent management system 10, according to an embodiment. Blockchain-based consent management system 10 according to this embodiment, is implemented using aspects of the hyperledger fabric framework (see, for example, https://www.hyperledger.org/projects/fabric). In this embodiment, a webserver subsystem 20 is configured to receive and handle authorized web user requests from users 5A, 5B, 5C, 5D and any other network participants for access to and/or transactions corresponding to consent data for a blockchain, as well as for access to other functionality not directly related to the blockchain. Webserver subsystem 20 includes a blockchain subsystem interface 40. Blockchain-based consent management system 10 also includes a blockchain subsystem 60 in communication with the blockchain subsystem interface 40 of webserver subsystem 20. In this embodiment, blockchain subsystem 60 defines a channel 62 having multiple organizations 64A, 64B, 64C etc., corresponding chaincode and an endorsement policy (not shown), each of the at least two organizations 64A, 64B etc. having, in this embodiment, multiple peers P. Each of the multiple peers P of organizations 64A, 64B etc. of channel 62 maintains a blockchain copy (not shown). In this embodiment, at least one peer P for each organization 64A, 64B etc. is designated as an anchor peer, enabling it to communicate with the anchor peer of another organization in the channel 62. In this embodiment, the bottom right peer P of organization 64A is an anchor peer and the top right peer P of organization 64B is an anchor peer. An orderer 80 of blockchain subsystem 60 is in communication with blockchain subsystem interface 40.

[0023] In operation, blockchain subsystem 60 and webserver subsystem 20 communicate such that authorized requests for transactions for the blockchain via a web application 22 cause webserver subsystem 20 to generate transaction proposals to be routed via the blockchain subsystem interface 40 to the channel peers P of the blockchain subsystem 60 for individual endorsement, and to receive endorsement responses from the peers P. In the event the endorsement responses collectively satisfy the endorsement policy, transmit the endorsed transactions to the orderer 80 for inclusion in an additional block of the blockchain. Furthermore, orderer 80 is configured to cause the additional block to be stored in each of the blockchain copy maintain by peers P.

[0024] Figure 2 is an enlarged schematic diagram showing components of webserver subsystem 20 of blockchain-based consent management system 10, according to this embodiment. Web

application 22, accessible through individual web browsers run on devices being used by network participants, provides authenticated access to webserver subsystem 20 for, in turn, providing access to the blockchain or for other functions not directly related to the blockchain.

[0025] In this embodiment, application 22 is deployed to web browser making requests of webserver subsystem 20 using HTTPs REST APIs (Hypertext Transfer Protocol, Representational State Transfer, Application Programming Interfaces), and is served from one of potentially several instances of a Node JS webserver 30 in an auto-scaling group of webserver subsystem 20. An auto-scaling group is a mechanism for enabling multiple instances of the Node JS webserver 30 to be instantiated or wound down, as required, to efficiently handle rises and falls in incoming traffic loads. A load balancing subsystem 24 for handling and distributing traffic, in this embodiment, includes an Amazon Route 53 DNS service 26 combined with an ELB (Elastic Load Balancer) 28.

[0026] The instance of the Node JS webserver 30 from which application 22 is served is representative of all members of its auto-scaling group, in that it provides an API interface 32, Auth Middleware 34, a Database Interface 38 and a Request Publisher 36. API interface 32 provides user interface code executable for deploying the user interface to users' web browsers for interacting with application 22 and interaction with a user for generating read requests, initiating transactions, and other operations. Auth Middleware 34 provides an interface to a Certificate Authority (CA) service. As would be understood, the CA service generates identifiers for each entity and participant in the network, particularly by issuing and maintaining cryptographically validated digital certificates complying with X.509 standard, thereby to authenticate and link identities such as peers P, organizations 64A, 64B, 64C etc., orderer 80, and the like. An MSP (Membership Service Provider) configuration is stored locally at each peer P and at orderer 80. Database Interface 38 provides controlled access to non-blockchain, security-related data maintained by a Security Group in, in this embodiment, a NoSQL DB 50 with caching support 52. The term Security Group is used to refer to Amazon's set of network security policies, as described in, for example, https://blog.learningtree.com/understanding-amazon-ec2-security-groups-and-firewalls.

[0027] Database Interface 38 also provides controlled access to a cloud storage service 54, in this embodiment an Amazon Simple Storage Service (Amazon S3), for storing supporting documentation and other data relating to consents being stored on the blockchain. For example, Amazon S3 54 will store deployment- and configuration-related assets, like Docker images of the Node JS webserver 40 that would be used to create new instances of it in its own auto scaling process.

[0028] Request Publisher 36 interfaces with a Request Queue RQ that is maintained by the Security Group in order to lodge requests, made in response to user requests provided via application 22.

[0029] A second auto-scaling group of Node JS webservers 40 is provided, primarily to serve as the blockchain subsystem interface. Each of Node JS webservers 40 in this second auto-scaling group includes a Request Consumer 42 that interfaces with the Request Queue RQ in order to draw off requests for further handling with respect to the blockchain. Each of Node JS webservers 40 also includes a respective Database Interface 46 for controlled access to non-blockchain, security-related data maintained by a Security Group in the NoSQL DB 50 with caching 52. Database Interface 46 also provides controlled access to the Amazon S3 cloud storage service 54. Node JS webserver 40 also interfaces with a Key Management System, in this embodiment Amazon KMS.

[0030] A Fabric Interface 44 enables Node JS webserver 40 to interface with blockchain subsystem 60. Figure 3 is an enlarged schematic diagram showing components of blockchain subsystem 60. In this embodiment, blockchain subsystem 60 is a hyperledger fabric instance maintaining a channel 62 particularly for handling storage, maintenance and access to consent data for participants in the network.

[0031] Channel 62 is a logical structure for managing a respective blockchain and enables the formation of a consortium around private data, such as the particular clients of a health information verification organization established to promote management of consents for and across the clients. In this embodiment, the consortium is shown to include two organizations 64A and 64B. Orderer 80 is, in this embodiment, a distributed Kafka and Zookeeper orderer service.

[0032] According to the hyperledger fabric framework, channel 62 has associated with it one or more chaincodes (smart contracts establishing business logic), corresponding endorsement policy(ies) and an access control list (ACL). In this embodiment, ACL implements a consent expiry check to block access to a consent after its respective expiry date. These channel attributes are each stored on each peer P whose organization 64A, 64B etc. has authorized the peer P for inclusion. Each organization in channel 62 may also be a part of another, different channel that maintains a different blockchain and is not affected by or accessible through channel 62. For example, in this example, organization 64A has its own chaincode and endorsement policies for a separate channel, and organization 64B has its own chaincode and endorsement policies for another, separate channel. Organizations 64A and 64B are, along with Other Organizations (64C, for example), also part of channel 62 in order to handle business logic corresponding to consent management with each other and any other organizations that may be added to the channel.

[0033] In this embodiment, a particular patient record is an asset in the blockchain of channel 62 and includes at least a portion of the data shown in Table 1, below:

asset Patient identified by id {
• String id • String firstname • String lastname • DateTime dob (date of birth) • String street1 • String street2 • String city • String state • String zip • String phone • String email
}

Table 1

[0034] In this embodiment, a particular consent record is an asset in the blockchain of channel 62 and includes at least a portion of the data shown in Table 2, below:

asset Consent identified by consentid {
• String consentid • String type • DateTime grant • DateTime expiry • Boolean status • String doc_type • String doc_id • String franchise • String brand • String program_name • String tactic • Strong channel
}

Table 2

[0035] In this embodiment, a particular patient consent is an asset in the blockchain of channel 62 and includes the contents of Table 3, below:

asset PatientConsent identified by PCid {
• String PCid ➔ Patient consentProvider ➔ Consents [] consents ➔ Grantee grantee
}

Table 3

[0036] In this embodiment, a consent grantee is a network participant of channel 62 identified according to Table 4, below:

participant Grantee identified by id {
• String id • String name
}

Table 4

[0037] Should a user make a request, made via application 22, to write a particular consent confirmation or other change to the blockchain, the chaincode for channel 62 is invoked on each peer P in channel 62 to trial the transaction through its respective blockchain copy and to provide an endorsement if the transaction would be acceptable to the peer P. In the event that the required endorsements provided back to the Fabric Interface 44 of the Node JS webserver 40 by peers P verify the endorsement policy for that chaincode has been satisfied, then the Fabric Interface 44 in turn interfaces with orderer 80 to provide an instruction to add the transaction to a next blockchain block. Pursuant to the instruction, orderer 80 orders the transactions into a new block and sends the new block to all organizations 64A, 64B, etc. in the channel to be added to respective copies of the blockchain maintained by peers P. As such, all peers P in the channel 62, even if from different organizations 64A, 64B etc., are meant to contain an accurate and up-to-date copy of the blockchain. Any other organizations with peers P in the channel 62 are similarly handled, and no other peers P or organizations that are not within channel 62 can access the blockchain of channel 62 either to read from it or write to it.

[0038] Various features are implemented using system 10, such as providing authorized users with the ability to search and view consents by different parameters, such as consent type, received date, expiry date referring to a date on which a consent, previously given, will expire, the individual's name, data of birth, ZIP or postal code, an identifier unique to the user or to the specific consent, and the consent status. Furthermore, system 10 enables an authorized user to update the status of a consent through its lifecycle from open, to pending approval, to approved, to expired, and so forth. System 10 also enables consents to be shared between and within enterprises according to chaincode and endorsement policies that correspond to proper and secure regulation of the respective consents.

[0039] In an embodiment, webserver subsystem 20 enables consent transactions to be manually loaded, batch loaded, or loaded using an automated mechanism from another system based on a scheduler. Consent data is stored in the blockchain, copies of which are maintained by each of the peers in a given channel to which the blockchain pertains.

[0040] In an embodiment, metadata corresponding to consents may be stored in the blockchain or otherwise securely stored, so that data supporting a consent or data proving a consent, such as an audio, video or image file including contents indicative of a patient's giving of the relevant consent, can be referred to for auditing or other regulatory purposes. For scalability, it may be preferred that such supporting documentation be stored separately, outside of the blockchain, from the consent data being stored within the blockchain.

[0041] In an embodiment, consents may be conveyed between entities in the system through appropriate authorizations, such as from a doctor to a subcontractor lab company doing lab work under the authorization of that doctor.

[0042] In an embodiment, various roles may be established for users accessing via the web application 22. For example, administrator users, read-only access, and the like. Furthermore, in embodiments, web application 22 deploys functionality enabling authorized users to add entities to the network, to add different kinds of consents and corresponding chaincodes and endorsement policies to the system, and to manage types of alerts (SMS, push notifications, emails) from within the system.

[0043] In an embodiment, both internal and external users of system 10 may be provided with the ability to be provided with information about the presence of a particular consent and/or to validate that a consent has been captured by system 10. Embodiments may provide alerts to designated users once a consent has changed status, such as when it has been captured, has been approved, or has expired, or has otherwise changed.

[0044] Embodiments log changes to consents throughout their lifecycles and provide user interface access to such logs and reporting tools so that consent lifecycles may be audited other otherwise explored.

[0045] Figure 2 is a schematic diagram showing a hardware architecture for one or more components of the blockchain-based consent management system 10 of Figure 1, according to an embodiment. As would be understood, components of blockchain-based consent management system 10 may be deployed using various load balancing schema, using cloud services such as Amazon Web Services (AWS), and the like, which themselves may deploy virtual servers to handle throughput on demand. Various implementations of the architecture using various techniques for load balancing, expansion, geographic locality, or the like, may be employed.

[0046] In an embodiment, computing system 1000 includes a bus 1010 or other communication mechanism for communicating information, and a processor 1018 coupled with the bus 1010 for processing the information. The computing system 1000 also includes a main memory 1004, such as a random access memory (RAM) or other dynamic storage device (e.g., dynamic RAM

(DRAM), static RAM (SRAM), and synchronous DRAM (SDRAM)), coupled to the bus 1010 for storing information and instructions to be executed by processor 1018. In addition, the main memory 1004 may be used for storing temporary variables or other intermediate information during the execution of instructions by the processor 1018. Processor 1018 may include memory structures such as registers for storing such temporary variables or other intermediate information during execution of instructions. The computing system 1000 further includes a read only memory (ROM) 1006 or other static storage device (e.g., programmable ROM (PROM), erasable PROM (EPROM), and electrically erasable PROM (EEPROM)) coupled to the bus 1010 for storing static information and instructions for the processor 1018.

[0047] Computing system 1000 also includes a disk controller 1008 coupled to the bus 1010 to control one or more storage devices for storing information and instructions, such as a magnetic hard disk 1022 and/or a solid state drive (SSD) and/or a flash drive, and a removable media drive 1024 (e.g., solid state drive such as USB key or external hard drive, floppy disk drive, read-only compact disc drive, read/write compact disc drive, compact disc jukebox, tape drive, and removable magneto-optical drive). The storage devices may be added to the computing system 1000 using an appropriate device interface (e.g., Serial ATA (SATA), peripheral component interconnect (PCI), small computing system interface (SCSI), integrated device electronics (IDE), enhanced-IDE (E-IDE), direct memory access (DMA), ultra-DMA, as well as cloud-based device interfaces).

[0048] Computing system 1000 may also include special purpose logic devices (e.g., application specific integrated circuits (ASICs)) or configurable logic devices (e.g., simple programmable logic devices (SPLDs), complex programmable logic devices (CPLDs), and field programmable gate arrays (FPGAs)).

[0049] While not strictly required for hardware that does not interact directly with users, computing system 1000 may also include a display controller 1002 coupled to the bus 1010 to control a display 1012, such as an LED (light emitting diode) screen, organic LED (OLED) screen, liquid crystal display (LCD) screen or some other device suitable for displaying information to a computer user. In embodiments, display controller 1002 incorporates a dedicated graphics processing unit (GPU) for processing mainly graphics-intensive or other highly-parallel operations. Such operations may include rendering by applying texturing, shading and the like to wireframe objects including polygons such as spheres and cubes thereby to relieve processor 1018 of having to undertake such intensive operations at the expense of overall performance of computing system 1000. The GPU may incorporate dedicated graphics memory for storing data generated during its operations, and includes a frame buffer RAM memory for storing processing results as bitmaps to be used to activate pixels of display 1012.

The GPU may be instructed to undertake various operations by applications running on computing system 1000 using a graphics-directed application programming interface (API) such as OpenGL, Direct3D and the like.

[0050] While not strictly required for hardware that does not interact directly with users, computing system 1000 may include input devices, such as a keyboard 1014 and a pointing device 1016, for interacting with a computer user and providing information to the processor 1018. The pointing device 1016, for example, may be a mouse, a trackball, or a pointing stick for communicating direction information and command selections to the processor 1018 and for controlling cursor movement on the display 1012. The computing system 1000 may employ a display device that is coupled with an input device, such as a touch screen. Other input devices may be employed, such as those that provide data to the computing system via wires or wirelessly, such as gesture detectors including infrared detectors, gyroscopes, accelerometers, radar/sonar and the like. A printer may provide printed listings of data stored and/or generated by the computing system 1000.

[0051] Computing system 1000 performs a portion or all of the processing steps discussed herein in response to the processor 1018 and/or GPU of display controller 1002 executing one or more sequences of one or more instructions contained in a memory, such as the main memory 1004. Such instructions may be read into the main memory 1004 from another processor readable medium, such as a hard disk 1022 or a removable media drive 1024. One or more processors in a multi-processing arrangement such as computing system 1000 having both a central processing unit and one or more graphics processing unit may also be employed to execute the sequences of instructions contained in main memory 1004 or in dedicated graphics memory of the GPU. In alternative embodiments, hard-wired circuitry may be used in place of or in combination with software instructions.

[0052] As stated above, computing system 1000 includes at least one processor readable medium or memory for holding instructions programmed according to the teachings of the invention and for containing data structures, tables, records, or other data described herein. Examples of processor readable media are solid state devices (SSD), flash-based drives, compact discs, hard disks, floppy disks, tape, magneto-optical disks, PROMs (EPROM, EEPROM, flash EPROM), DRAM, SRAM, SDRAM, or any other magnetic medium, compact discs (e.g., CD-ROM), or any other optical medium, punch cards, paper tape, or other physical medium with patterns of holes, a carrier wave (described below), or any other medium from which a computer can read.

[0053] Stored on any one or on a combination of processor readable media, is software for controlling the computing system 1000, for driving a device or devices to perform the functions discussed herein, and for enabling computing system 1000 to interact with a human user. Such software

may include, but is not limited to, device drivers, operating systems, development tools, and applications software. Such processor readable media further includes the computer program product for performing all or a portion (if processing is distributed) of the processing performed discussed herein.

[0054] The computer code devices discussed herein may be any interpretable or executable code mechanism, including but not limited to scripts, interpretable programs, dynamic link libraries (DLLs), Java classes, and complete executable programs. Moreover, parts of the processing of the present invention may be distributed for better performance, reliability, and/or cost.

[0055] A processor readable medium providing instructions to a processor 1018 may take many forms, including but not limited to, non-volatile media, volatile media, and transmission media. Non-volatile media includes, for example, optical, magnetic disks, and magneto-optical disks, such as the hard disk 1022 or the removable media drive 1024. Volatile media includes dynamic memory, such as the main memory 1004. Transmission media includes coaxial cables, copper wire and fiber optics, including the wires that make up the bus 1010. Transmission media also may also take the form of acoustic or light waves, such as those generated during radio wave and infrared data communications using various communications protocols.

[0056] Various forms of processor readable media may be involved in carrying out one or more sequences of one or more instructions to processor 1018 for execution. For example, the instructions may initially be carried on a magnetic disk of a remote computer. The remote computer can load the instructions for implementing all or a portion of the present invention remotely into a dynamic memory and send the instructions over a wired or wireless connection using a modem. A modem local to the computing system 1000 may receive the data via wired Ethernet or wirelessly via Wi-Fi and place the data on the bus 1010. The bus 1010 carries the data to the main memory 1004, from which the processor 1018 retrieves and executes the instructions. The instructions received by the main memory 1004 may optionally be stored on storage device 1022 or 1024 either before or after execution by processor 1018.

[0057] Computing system 1000 also includes a communication interface 1020 coupled to the bus 1010. The communication interface 1020 provides a two-way data communication coupling to a network link that is connected to, for example, a local area network (LAN) 1500, or to another communications network 2000 such as the Internet. For example, the communication interface 1020 may be a network interface card to attach to any packet switched LAN. As another example, the communication interface 1020 may be an asymmetrical digital subscriber line (ADSL) card, an integrated services digital network (ISDN) card or a modem to provide a data communication

connection to a corresponding type of communications line. Wireless links may also be implemented. In any such implementation, the communication interface 1020 sends and receives electrical, electromagnetic or optical signals that carry digital data streams representing various types of information.

[0058] The network link typically provides data communication through one or more networks to other data devices, including without limitation to enable the flow of electronic information. For example, the network link may provide a connection to another computer through a local network 1500 (e.g., a LAN) or through equipment operated by a service provider, which provides communication services through a communications network 2000. The local network 1500 and the communications network 2000 use, for example, electrical, electromagnetic, or optical signals that carry digital data streams, and the associated physical layer (e.g., CAT 5 cable, coaxial cable, optical fiber, etc.). The signals through the various networks and the signals on the network link and through the communication interface 1020, which carry the digital data to and from the computing system 1000, may be implemented in baseband signals, or carrier wave based signals. The baseband signals convey the digital data as unmodulated electrical pulses that are descriptive of a stream of digital data bits, where the term "bits" is to be construed broadly to mean symbol, where each symbol conveys at least one or more information bits. The digital data may also be used to modulate a carrier wave, such as with amplitude, phase and/or frequency shift keyed signals that are propagated over a conductive media, or transmitted as electromagnetic waves through a propagation medium. Thus, the digital data may be sent as unmodulated baseband data through a "wired" communication channel and/or sent within a predetermined frequency band, different than baseband, by modulating a carrier wave. The computing system 1000 can transmit and receive data, including program code, through the network(s) 1500 and 2000, the network link and the communication interface 1020. Moreover, the network link may provide a connection through a LAN 1500 to a mobile device 1300 such as a personal digital assistant (PDA) laptop computer, or cellular telephone.

[0059] Alternative configurations of computing systems may be used to implement the systems and processes described herein.

[0060] Electronic data stores implemented in the database described herein may be one or more of a table, an array, a database, a structured data file, an XML file, or some other functional data store, such as hard disk 1022 or removable media 1024.

[0061] Although embodiments have been described with reference to the drawings, those of skill in the art will appreciate that variations and modifications may be made without departing from the spirit, scope and purpose of the invention as defined by the appended claims.

[0062] For example, in an embodiment, a single entity may store all peer instances thereby centrally storing all copies of the blockchain. The peer instances may control access to respective blockchains, but they may be stored either physically or logically in a central manner rather than physically distributed as different machines.

[0063] In another embodiment, some of the peers are stored centrally and some are physically different machines.

[0064] In another embodiment, all peers are physically different machines. In an embodiment, transactions may be routed, based on access control, to the peers using an interface other than the application.

[0065] In an embodiment, organizations manage their own cryptographic blockchain identities, using them to sign transactions such as creating or updating consent before sending the transactions to the web application. This architecture may increase the certainty that data is being provided to system by an authorized party.

[0066] In an embodiment, the web application provides different levels of access control so that certain users within an organization can have modified or restricted access to data stored on the blockchain, according to the roles and responsibilities within the organization.

What is claimed is:

1. A blockchain-based consent management system comprising:

a webserver subsystem configured to receive and handle authorized web user requests for access to and/or transactions corresponding to consent data for a blockchain, the webserver subsystem comprising a blockchain subsystem interface; and

a blockchain subsystem defining a channel having at least two organizations, corresponding chaincode and an endorsement policy, each of the at least two organizations having at least one peer, each of the at least one peer maintaining a blockchain copy, the blockchain subsystem comprising an orderer in communication with the blockchain subsystem interface.

2. The blockchain-based consent management system of claim 1, wherein the blockchain subsystem and the webserver subsystem communicate such that authorized requests for transactions for the blockchain cause the webserver subsystem to generate transaction proposals to be routed via the blockchain subsystem interface to the channel peers of the blockchain subsystem for individual endorsement, to receive endorsement responses from the peers, and to, in the event the endorsement responses collectively satisfy the endorsement policy, transmit the endorsed transactions to the orderer for inclusion in an additional block of the blockchain,

wherein the orderer is configured to cause the additional block to be stored in each of the peers' blockchain copy.

3. The blockchain-based consent management system of claim 1, wherein the webserver subsystem is in communication with a certificate authority.

4. The blockchain-based consent management system of claim 1, wherein the webserver subsystem comprises a first auto-scaling group in communication with a second auto-scaling group via a request queue, wherein the first auto-scaling group lodges requests corresponding to user requests in the request queue for consumption by the second auto-scaling group.

5. The blockchain-based consent management system of claim 3, wherein the first auto-scaling group comprises one or more Node JS webservers having user interface and application middleware components.

6. The blockchain-based consent management system of claim 3, wherein the second auto-scaling group comprises one or more Node JS webservers having instances of a hyperledger fabric interface.

7. The blockchain-based consent management system of claim 3, wherein the webserver subsystem further comprises load balancing components for routing the user requests to webserver instances in the first auto-scaling group.

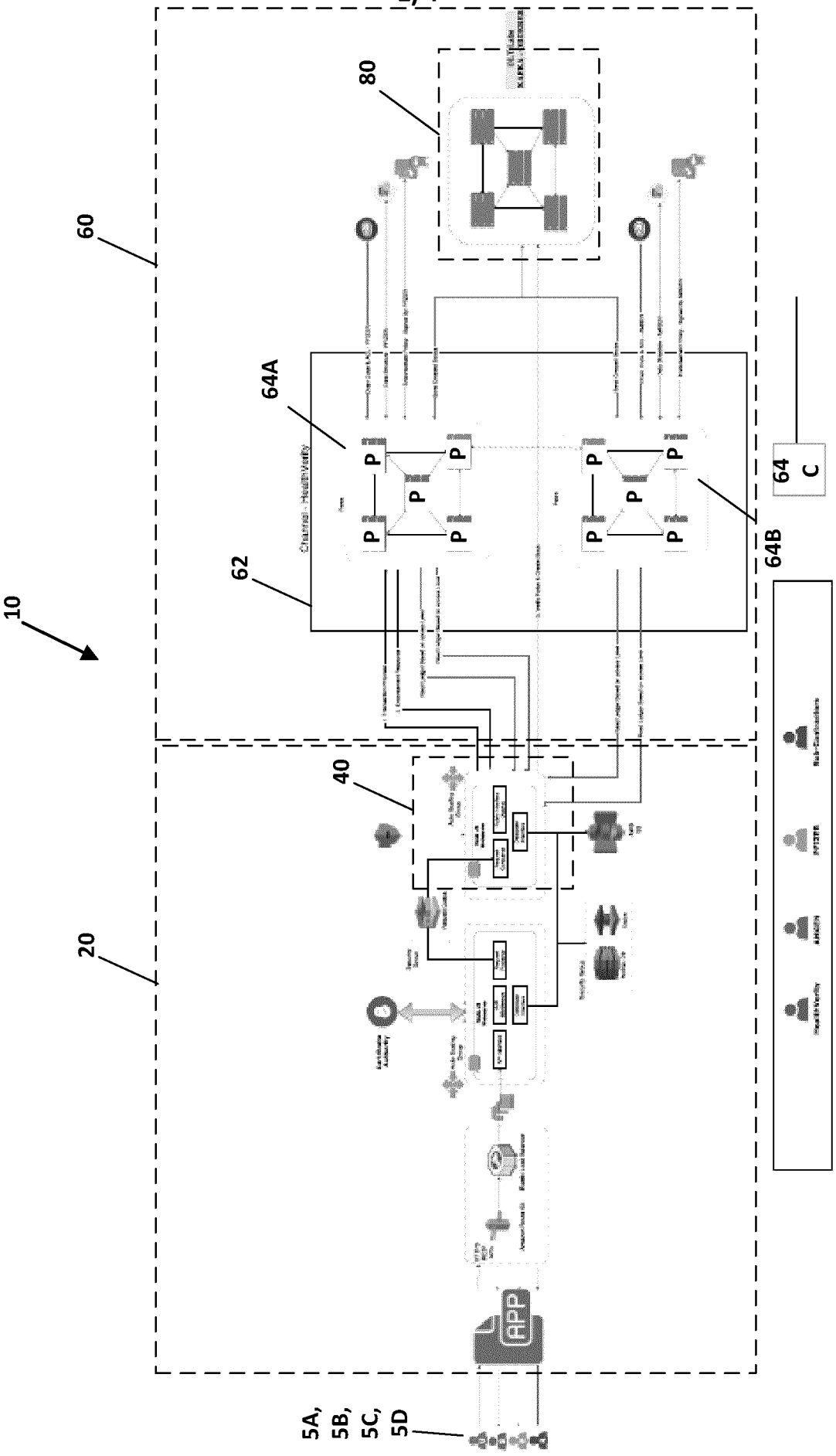


Fig. 1

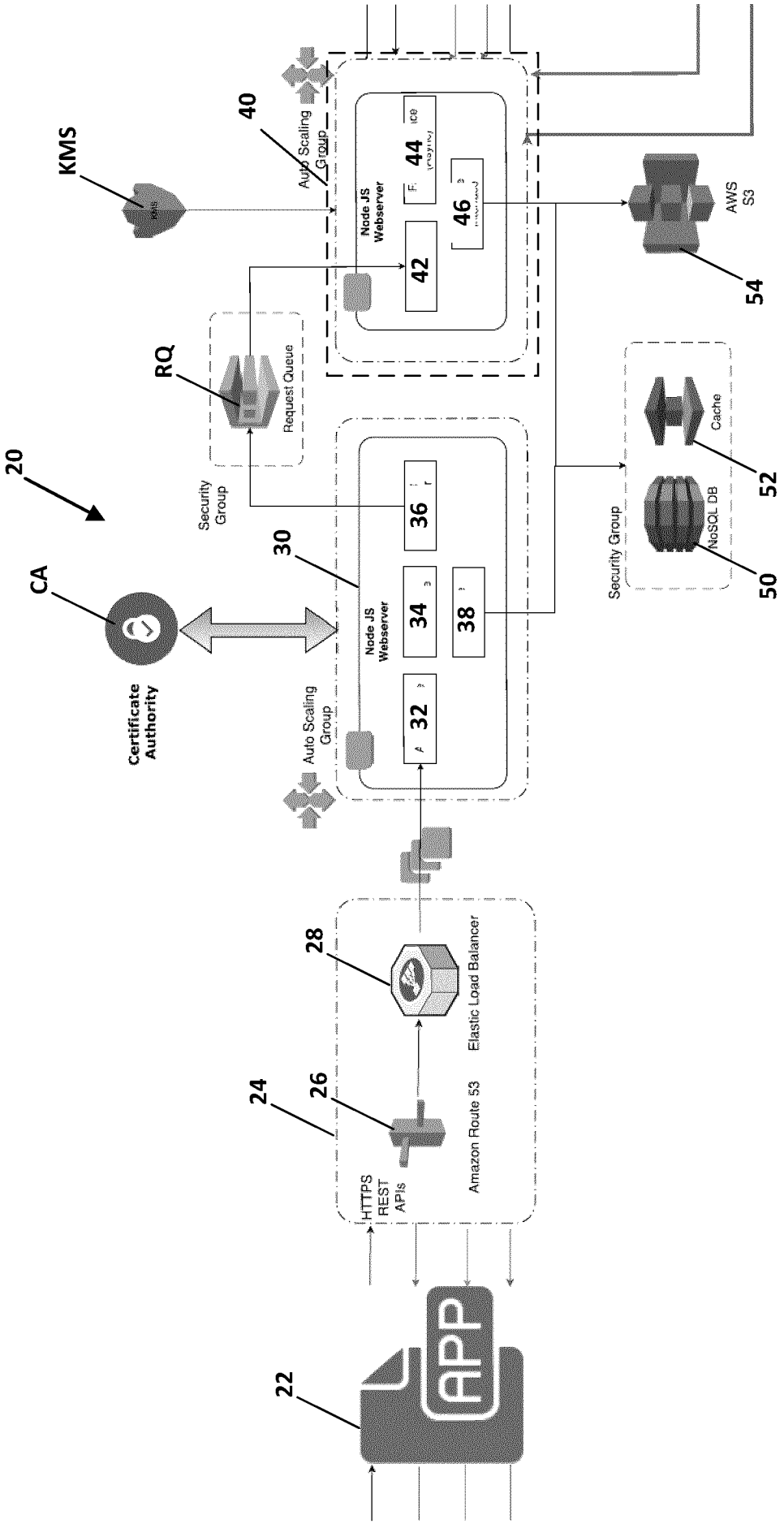

20
22
APP
24
HTTPS REST APIs
26
Amazon Route 53
28
Elastic Load Balancer
30
Auto Scaling Group
Node JS Webserver
32
34
36
38
CA
Certificate Authority
RQ
Request Queue
Security Group
40
Auto Scaling Group
Node JS Webserver
42
44
46
KMS
AWS S3
54
Cache
52
NoSQL DB
50
Security Group

Fig. 2

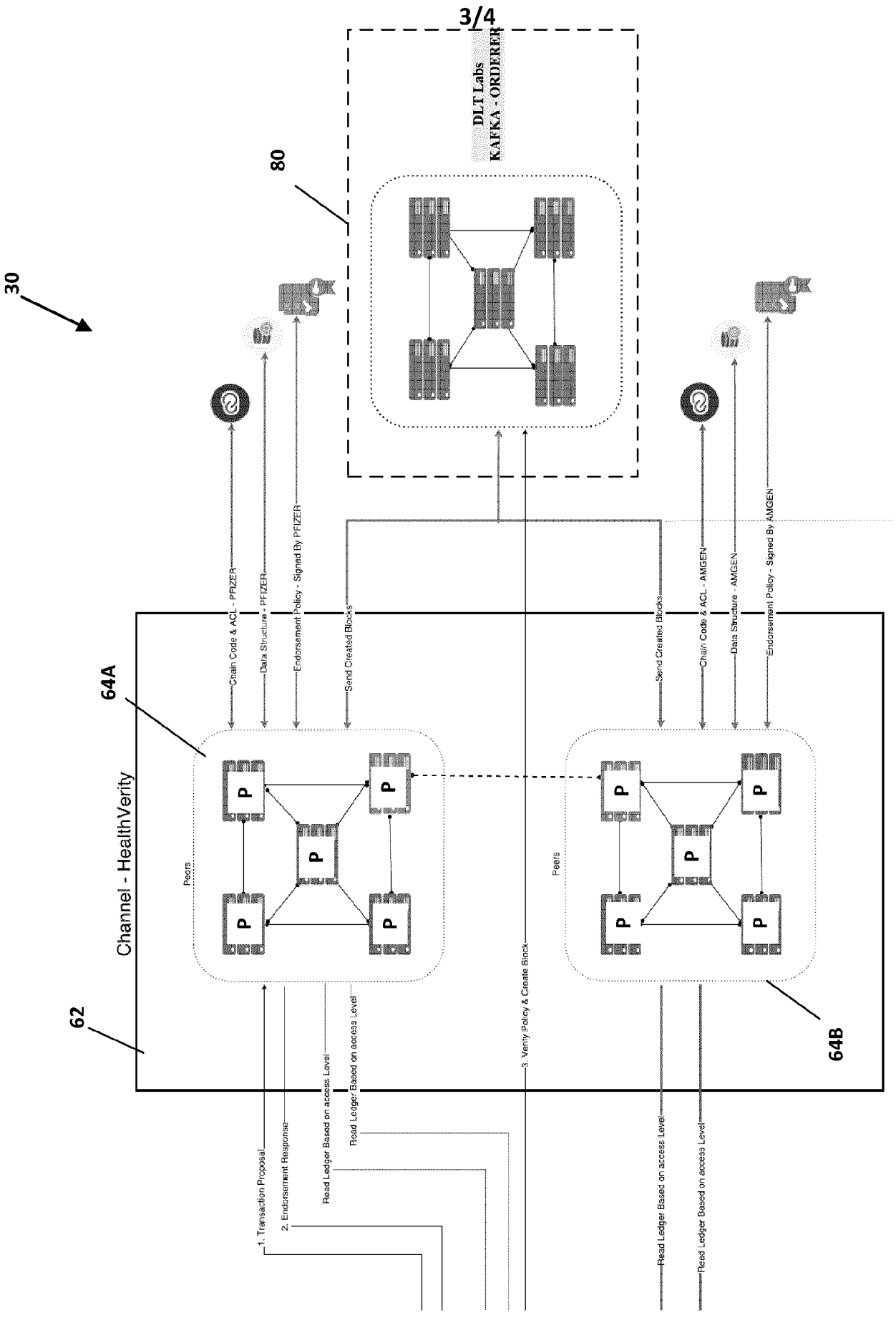

3/4
30
80
DLT Labs
KAFKA - ORDERER
64A
64B
62
Channel - HealthVerity
Peers
Peers
P
Chain Code & ACL - PFIZER
Data Structure - PFIZER
Endorsement Policy - Signed By PFIZER
Send Created Blocks
Send Created Blocks
Chain Code & ACL - AMGEN
Data Structure - AMGEN
Endorsement Policy - Signed By AMGEN
1. Transaction Proposal
2. Endorsement Response
Read Ledger Based on access Level
Read Ledger Based on access Level
3. Verify Policy & Create Block
Read Ledger Based on access Level
Read Ledger Based on access Level

Fig. 3

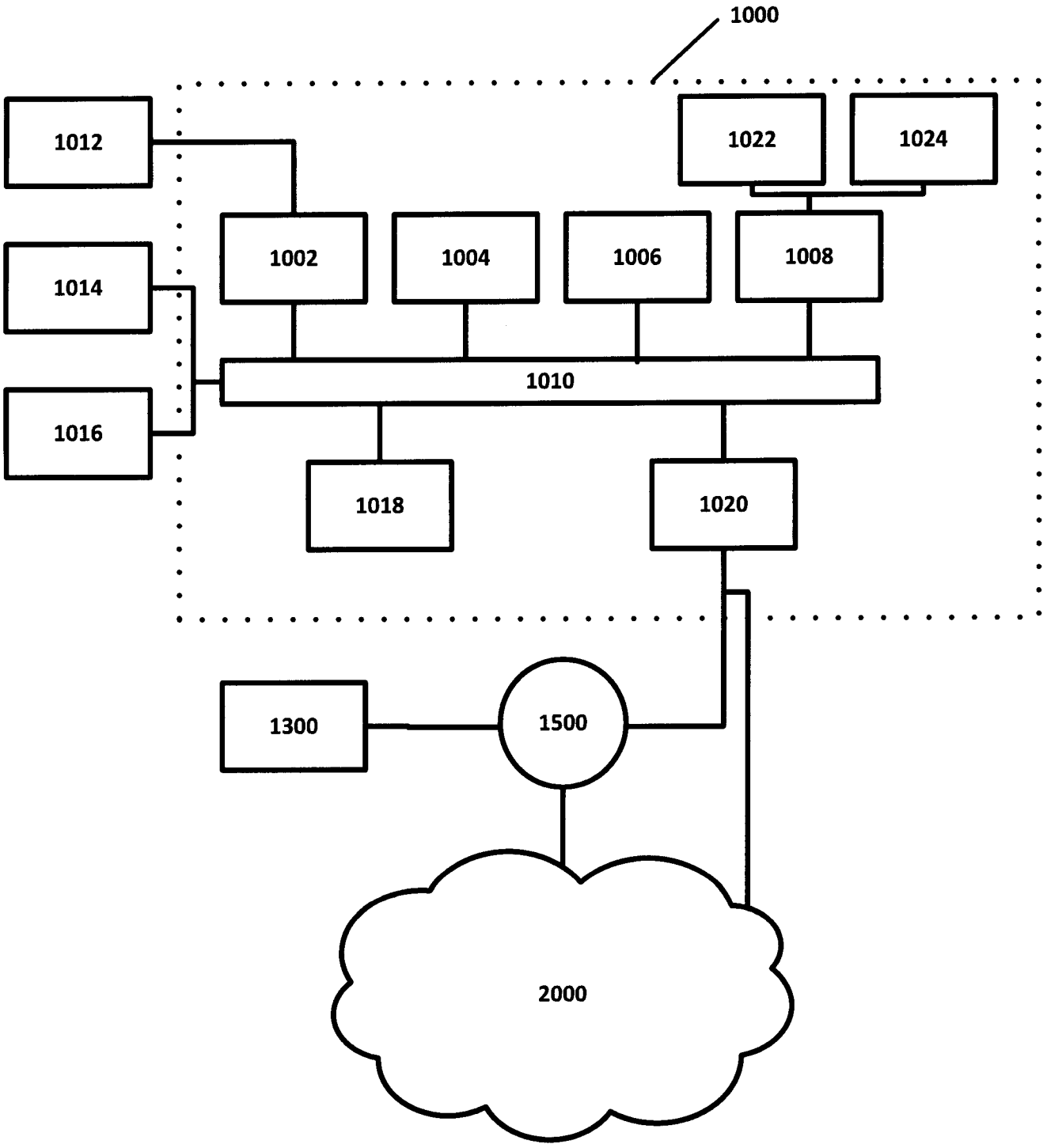

1000
1012
1022
1024
1002
1004
1006
1008
1014
1010
1016
1018
1020
1300
1500
2000

Fig. 4

Fig. 1