



(51) International Patent Classification:
G06Q 50/22 (2012.01)

(21) International Application Number:
PCT/FI2016/050572

(22) International Filing Date:
22 August 2016 (22.08.2016)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **NOKIA TECHNOLOGIES OY** [FI/FI];
Karaportti 3, 02610 Espoo (FI).

(72) Inventors: **ROENNOW, Troels F.**; 61 Ellis Road, Cambridge CB2 9BG (GB). **ISOPOUSSU, Anton**; 8, Clare Street, Cambridge CB4 3BY (GB). **SAVOLAINEN, Teemu Ilmari**; Manttaalimutka 18 B4, FI-37120 Nokia (FI).

(74) Agent: **ESPATENT OY**; Kaivokatu 10 D, 00100 Helsinki (FI).

(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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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).

Declarations under Rule 4.17:

— of inventorship (Rule 4.17(iv))

Published:

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

(54) Title: METHOD AND APPARATUS FOR BLOCKCHAIN VERIFICATION OF HEALTHCARE PRESCRIPTIONS

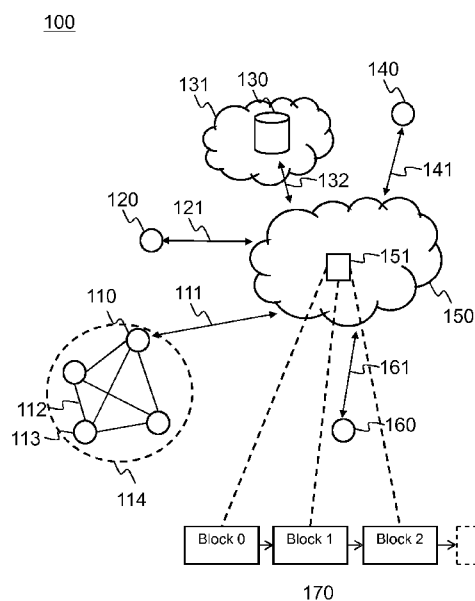


Fig. 1

(57) Abstract: A computer-implemented method for blockchain verification of healthcare prescriptions, the method comprising generating a prescription data item by a first user authorized to generate the prescription data item; associating the prescription data item to a first transaction; recording the first transaction to a blockchain, the first transaction transferring ownership of the prescription data item to a second user; recording a second transaction to the blockchain, the second transaction transferring ownership of at least part of the prescription data item to a third user; modifying the prescription data item by the third user; and recording a third transaction to the blockchain, the third transaction transferring ownership of the modified prescription data item to the first user, the second user or a fourth user.

METHOD AND APPARATUS FOR BLOCKCHAIN VERIFICATION OF HEALTHCARE PRESCRIPTIONS

TECHNICAL FIELD

[0001] The present application generally relates to blockchains, distributed databases, distributed ledgers, and cryptographic protocols. Furthermore, the present application relates to generating and storing health records and healthcare prescriptions.

BACKGROUND

[0002] This section illustrates useful background information without admission of any technique described herein representative of the state of the art.

[0003] Today, medical prescriptions are handled differently in different countries. This means that a prescription given in first country is not usually valid in second country. People moving across the border have difficulties when trying to get medicine from pharmacy of second country for which they have prescription in first country. This is due incompatible systems and difficulties in second country to validate prescriptions given by doctor of the first country (difficulties are caused by lack of information, trust, and legislation). For a patient visiting another country it may be a problem to know which pharmacies can be trusted to give valid medicines.

[0004] Furthermore, use of centralized prescription system per country increases global costs due multiple implementations of prescription management system – every country has to pay and arrange their own systems. Paper based prescriptions are difficult to track for misuse, such as fake doctors issuing prescriptions or real doctors prescribing too much or single person getting too many prescriptions from multiple doctors. Paper based prescriptions may also be subject to forgery.

[0005] Thus, a technical solution is needed to solve problems of how to allow use of prescriptions across country boundaries, how to save in costs required to build and maintain prescription databases and how to minimize misuse possibilities (which may cause even death or support crimes).

SUMMARY

[0006] Various aspects of examples of the invention are set out in the claims.

[0007] According to a first example aspect of the present invention, there is provided a computer-implemented method for blockchain verification of healthcare prescriptions, the method comprising:

generating a prescription data item by a first user authorized to generate the prescription data item;

associating the prescription data item to a first transaction;

recording the first transaction to a blockchain, the first transaction transferring ownership of the prescription data item to a second user;

recording a second transaction to the blockchain, the second transaction transferring ownership of at least part of the prescription data item to a third user;

modifying the prescription data item by the third user; and

recording a third transaction to the blockchain, the third transaction transferring ownership of the modified prescription data item to the first user, the second user or a fourth user.

[0008] In an embodiment, the method further comprises:

signing the prescription data item by a fourth user in response to recording the first transaction to the blockchain; and

recording the second transaction to the blockchain in response to signing the prescription data item by the fourth user.

[0009] In an embodiment,

the first user being a doctor prescribing the prescription data item;

the second user being a patient the prescription data item being prescribed for;

the third user being a certified pharmacist; and

the fourth user being an administrator.

[0010] In an embodiment, the method further comprises:

determining received prescription information by the third user, the received prescription information corresponding to medicines received by the second user; and

modifying the prescription data item by the third user based on the received prescription information.

[0011] In an embodiment, the method further comprises:

defining a blockchain record comprising certified first users.

[0012] In an embodiment, the method further comprises:

defining a blockchain record comprising certified third users.

[0013] In an embodiment, the method further comprises:
defining a blockchain record comprising certified fourth users.

[0014] In an embodiment, the first transaction comprises an identifier of the second user; a hash value of the prescription data item; and a public key of the first user.

[0015] In an embodiment, the method further comprises:
signing the prescription data item by the first user; and
recording the signed prescription data item as a transaction to the blockchain in response to signing the prescription data item by the first user.

[0016] In an embodiment, the method further comprises:
receiving, by the second user, a challenge from the third user to verify an identity of the second user.

[0017] In an embodiment, the method further comprises:
signing, by the second user, a previous blockchain record issued by the first user to verify identity of the second user.

[0018] In an embodiment, the method further comprises:
generating a third transaction, by the third user, to invalidate at least part of the prescription data item.

[0019] In an embodiment, the method further comprises:
signing the third transaction by the third user and the second user.

[0020] In an embodiment, at least one of the first, second or third transaction is added as a next block to the blockchain according to a consensus algorithm.

[0021] In an embodiment, the method further comprises:
receiving a certificate of a first user;
verifying that the certificate being authorized for generating the prescription data item; and
in response to successful authorization, recording the first transaction to the blockchain, the first transaction transferring ownership of the prescription data item to the second user.

[0022] In an embodiment, the method further comprises:
assigning a node identifier to each node of the first, the second and the third user.

[0023] In an embodiment, the node identifier comprises a public key.

[0024] In an embodiment, the first, the second and the third user are connected

to a wide area communication interface.

[0025] In an embodiment, the blockchain is configured to be protected by a proof algorithm comprising at least one of a proof-of-work, proof-of-stake and majority-voting algorithm.

[0026] According to a second example aspect of the present invention, there is provided an apparatus comprising:

- a communication interface for transceiving information;

- at least one processor; and

- at least one memory including computer program code;

the at least one memory and the computer program code configured to, with the at least one processor, cause the apparatus to:

- generate a prescription data item by a first user authorized to generate the prescription data item;

- associate the prescription data item to a first transaction;

- record the first transaction to a blockchain, the first transaction transferring ownership of the prescription data item to a second user;

- record a second transaction to the blockchain, the second transaction transferring ownership of at least part of the prescription data item to a third user;

- modify the prescription data item by the third user; and

- record a third transaction to the blockchain, the third transaction transferring ownership of the modified prescription data item to the first user, the second user or a fourth user.

[0027] In an embodiment, the apparatus comprises a plurality of user devices operated by at least two of the first user, the second user, the third user and the fourth user.

[0028] According to a third example aspect of the present invention, there is provided computer program embodied on a computer readable non-transitory medium comprising computer executable program code, which when executed by at least one processor of a apparatus, causes the apparatus to:

- generate a prescription data item by a first user authorized to generate the prescription data item;

- associate the prescription data item to a first transaction;

- record the first transaction to a blockchain, the first transaction transferring

ownership of the prescription data item to a second user;

record a second transaction to the blockchain, the second transaction transferring ownership of at least part of the prescription data item to a third user;

modify the prescription data item by the third user; and

record a third transaction to the blockchain, the third transaction transferring ownership of the modified prescription data item to the first user, the second user or a fourth user.

[0029] Different non-binding example aspects and embodiments of the present invention have been illustrated in the foregoing. The embodiments in the foregoing are used merely to explain selected aspects or steps that may be utilized in implementations of the present invention. Some embodiments may be presented only with reference to certain example aspects of the invention. It should be appreciated that corresponding embodiments may apply to other example aspects as well.

BRIEF DESCRIPTION OF THE DRAWINGS

[0030] For a more complete understanding of example embodiments of the present invention, reference is now made to the following descriptions taken in connection with the accompanying drawings in which:

[0031] Fig. 1 shows a schematic drawing of a system of an example embodiment;

[0032] Fig. 2 shows another schematic drawing of a system of an example embodiment;

[0033] Fig. 3 shows a flow diagram illustrating a method according to an example embodiment of the invention;

[0034] Fig. 4 shows a block diagram of a device or apparatus of an example embodiment; and

[0035] Fig. 5 shows a block diagram of a server apparatus of an example embodiment.

DETAILED DESCRIPTION OF THE DRAWINGS

[0036] Example embodiments of the present invention and its potential advantages are understood by referring to Figs. 1 through 5 of the drawings. In this document, like reference signs denote like parts or steps.

[0037] In this document, the terms couple and connect may refer to direct contact between components or to coupling through some intervening component(s).

[0038] This application is related to distributed ledgers, blockchains and databases. It is further related storing health records, medical prescriptions and cloud security. It is also related to cryptocurrencies. Blockchains are technology that enables tamper-proof timestamped distributed databases. Cryptographic signatures and data encryption enable the level of security required for healthcare data.

[0039] A block chain is a distributed database that maintains a continuously growing list of data records hardened against tampering and revision. It consists of data structure blocks, which hold exclusively data in initial block chain implementations, and both data and programs in some implementations, with each block holding batches of individual transactions and the results of any block chain executables. Each block contains a timestamp and information linking it to a previous block.

[0040] The block chain is seen as the main technical innovation of bitcoin, where it serves as the public ledger of all bitcoin transactions. Bitcoin is peer-to-peer, every user is allowed to connect to the network, send new transactions to it, verify transactions, and create new blocks, which is why it is called permissionless. This original design has been the inspiration for other cryptocurrencies and distributed databases.

[0041] The medical prescriptions can be written to paper by doctor, possibly including for example doctor's name, institute, doctor's registration number, seal of sorts, and written signature, for example. The prescriptions may also be given verbally by doctor over a phone call to pharmacy. In more modern approaches, the prescriptions may be electronic and utilize centralized databases (e-prescription) stored in database managed by a trusted institution. Doctors can access the database to add prescriptions, and pharmacies can then access this database when giving medicines to people, and people may access this database to see what prescriptions doctors have given to them. Government will be able to track prescriptions and get statistics out of this database. However, such system is expensive.

[0042] Fig. 1 shows a schematic drawing of a system 100 of an example embodiment.

[0043] At the minimum, the system 100 comprises at least one node 110, 120,

140, 160 for transceiving data within the system 100. The node 110, 120, 140, 160 may comprise a user device, an IoT (Internet of Things) device, a sensor, an integrated device or home electronics device, for example. The user device may comprise a portable electronic device, a smartphone, a PDA, a tablet, a laptop computer, a wrist-based device, a belt device, clothing-integrated device, skin-attached sensor, or a separate personal health device such as a thermometer or a blood pressure meter, a heart rate monitor, a blood sugar level sensor, a lactate level sensor, and an oxygen saturation sensor, for example.

[0044] In an embodiment, a block chain infrastructure may be utilized to define a trusted circle 114 comprising at least two nodes 110, 113 of a plurality of nodes.

[0045] The system 100 illustrates nodes 110, 120, 140, 160 in a healthcare network that are configured or programmed to manage healthcare transactions in the form of a blockchain 170. Each block in the chain 170 includes one or more healthcare transactions that further incorporate information representing transaction information by nodes 110, 120, 140, 160. In some embodiments, the nodes operate collectively in a peer-to-peer network. Further a node 113 can exist within a trusted circle 114 of nodes, such as a clinical ecosystem or a patient ecosystem, for example.

[0046] In an embodiment, a node represents an entity that has a stake in a healthcare management process. The node could correspond to a patient, a doctor, a nurse, a technician, a care provider, a guardian, a parent, a broker, or other individual. Further, the node could also include other types of entities including a company, an affiliation, a hospital, an organization, a demographic, a community, or other type of entity.

[0047] In an embodiment, a blockchain 170 represents a chronicle or ledger (public ledger, private ledger, protected ledger, for example) of healthcare transactions for a prescription data item. With respect to a patient, the blockchain 170 might start with an initial block or genesis block created at birth that includes information associated with the patient's birth. Alternatively, the initial block may be created when the patient enters the healthcare system for prescription for the first time. Each subsequent healthcare transaction for the patient can be combined with the blockchain 170 as a new block, possibly until the blockchain 170 becomes eventually terminated when the patient exits the healthcare system.

[0048] In an embodiment, a blockchain 170 represents a chronicle or ledger

(public ledger, private ledger, protected ledger, for example) of healthcare transactions of a plurality of users for prescription data items. With respect to patients, the blockchain 170 might start with an initial block or genesis block. The initial block may be created when a patient enters the healthcare system for prescription for the first time, for example. Each subsequent healthcare transaction for the patients can be combined with the single blockchain 170 as a new block.

[0049] In an embodiment, a blockchain 170 could comprise any number of blocks. For a healthy patient, the blockchain 170 might only increase in size by one block per year based on an annual visit to a doctor, for example.

[0050] In an embodiment, there is provided a computer-implemented method for blockchain verification of healthcare prescriptions. A first node 110 operated by a first user may generate a prescription data item 151, wherein the first user of the first node 110 is authorized to generate the prescription data item 151. The prescription data item 151 may be associated to a first transaction. The first transaction may be recorded to a blockchain 170, the first transaction transferring ownership of the prescription data item 151 to a second user 120. A second transaction may be recorded to the blockchain 170, the second transaction transferring ownership of at least part of the prescription data item 151 to a third user 160. The prescription data item 151 may be modified by the third user 160 and a third transaction may be recorded to the blockchain 170, the third transaction transferring ownership of the modified prescription data item 151 to the first user 110, the second user 120 or a fourth user 140. The data item 151 is placed to the network 150 for illustrative purposes only. In practice the data item 151 is transceived within the system 100 nodes.

[0051] In an embodiment, the prescription data item may be signed by a fourth user 140 in response to recording the first transaction to the blockchain 170 and the second transaction being recorded to the blockchain 170 in response to signing the prescription data item by the fourth user 140.

[0052] In an embodiment, the first user is a doctor prescribing the prescription data item; the second user is a patient the prescription data item being prescribed for; the third user is a certified pharmacist; and the fourth user is an administrator.

[0053] In an embodiment, a first node 110 may receive a notification information identifying a trusted user circle 114 comprising the first node 110 and a second node 113, wherein the first node 110 and the second node 113 are configured to define a

private blockchain 170. Private block chain data is maintained within the trusted user circle 114 according to pre-defined settings, wherein the private block chain data is divided between nodes 110, 113 of the trusted user circle 114 based on the pre-defined settings.

[0054] In an embodiment, nodes correspond to devices. Thus, devices may be paired and in response to pairing the devices collaborate on storing and securing the contents of a distributed ledger. This technique enables, for example, home devices with little storage (such as general IoT nodes) to collaborate on forming one “super” node corresponding to the trusted user circle with capacity similar to that of an ordinary node hosted on a PC or in a cloud. Furthermore also other resources may be shared within the trusted user circle, such as hashing power, or listing of peers, for example.

[0055] Any node 110, 120, 140, 160 may generate transaction data relating to the node and hash the data using a cryptographic hashing function, to create a cryptographic hash block.

[0056] In an embodiment, the trusted user circle 114 may comprise a gateway node 110 configured to control access of other nodes within the trusted user circle 114 to external network 150 outside the trusted user circle 114. Node 110 may be for example a doctor responsible for prescriptions and node 113 a nurse preparing preliminary prescription data item for verification and approval for the doctor, for example.

[0057] In an embodiment, the gateway node may receive data without hashing from other nodes within the trusted user circle and carry out the data hashing using a cryptographic hashing function, to create a cryptographic hash block.

[0058] Nodes 110, 120, 140, 160 may communicate with other nodes within the system 100. The node may be connected to a public network 150 over connection 111, 121, 141, 161.

[0059] In an embodiment, the nodes are integrated as a single device. Alternatively, the gateway node 110 and another node 113 are separate entities and connected via a local short-range communication interface 112, and the gateway node 110 and a remote node 140 are connected via a wide area communication interface 150, for example. It is also possible to arrange the nodes to be releasably connectable to each other so that in one operating mode they are integrated together and in second operating mode they are separate entities.

[0060] After hashing, the node 110, 120, 140, 160 is configured to record the cryptographic hash block associated with a digital signature to a block of a blockchain 170.

[0061] In an embodiment, transaction data may be encrypted before hashing. For example, asymmetrical encrypting of the data may be carried out by the node 110, 120, 140, 160. The encrypted data may be stored to at least one of the nodes 110, 120, 140, 160, to the blockchain 170, to the central database 130, to the distributed database, or other parts of the system 100.

[0062] An owner of blockchain nodes 110, 120, 140, 160 may have many nodes (as for instance could be the case in IoT). While the owner may not trust any device he does not own, he may trust his own devices. Thus a trusted circle of nodes 114 may be established.

[0063] In an embodiment, the nodes 110, 120, 140, 160 are configured to generate transaction data and further take care of encrypting the data if needed, as well as hashing the data using a cryptographic hashing function, to create a cryptographic hash block, to record the cryptographic hash block associated with a digital signature of a node 110, 120, 140, 160 to a block of a digital blockchain 170 and to transmit the data item to a peer node, for example.

[0064] The local short-range communication interface 111, 112, 121, 141, 161 may comprise wired or wireless interface. The wide area communication interface may comprise a public network 150, such as Internet.

[0065] In an embodiment, the first node 110 and the second node 113 may be implemented as separate devices communicating with each other over a local connection 112. The local connection 112 may comprise also other wireless non-cellular connection. The wireless non-cellular connection may comprise industrial, scientific and medical (ISM) radio bands that are radio bands (portions of the radio spectrum) reserved internationally for the use of radio frequency (RF) energy for industrial, scientific and medical purposes, for example. Alternatively, the first node 110 may be comprised by the second node 113. The trusted circle 114 may also correspond to a system within user's home, wherein the first node and the second node communicate with each other over a local connection 112.

[0066] In an embodiment, a communication interface module of at least one of the nodes 110, 120, 140, 160 may comprise location modules for tracking location information of the node. Such location modules may comprise a module for providing

a connection to satellite based global positioning system (e.g. GPS), a module for cellular based positioning system, a module for indoor positioning, a module for wireless non-cellular positioning system (e.g. Wi-Fi) or a module for hybrid positioning system, for example.

[0067] In an embodiment, a node may be connected over a wireless or wired connection to a wide area network 150, such as Internet. Router apparatuses (not shown) may be used for providing the access to a wide area network 150. The access may comprise cellular or non-cellular connection.

[0068] In an embodiment, the system 100 comprises a server apparatus 130, which comprises a storage device for example for storing and providing user data, service data and subscriber information, over data connection 132. The service data may comprise configuration data, account creation data, prescription data, transaction data of the nodes, and digital block chain data, for example.

[0069] In an embodiment, a proprietary application in the node 110, 120, 140, 160 may be a client application of a service whose server application is running on the server apparatus 130 of the system 100. The proprietary application may capture or process transaction data for the service and provide the transaction data hashing, blockchain recording and transceiving for the service. In an embodiment, information between nodes 110, 120, 140, 160 and/or the server 130 is transceived via the connections 111, 121, 132, 141, 150, 161 automatically. Thus the user of the nodes may not need to do any control for the service. The system server 130 may also maintain account creation process details for the service, such as attaching new nodes to the system 100 as well as maintaining authorized users and devices.

[0070] In an embodiment, history data of earlier transaction data, user profiles, settings, agreements, prescription data, smart contracts, and blockchains may be maintained at the server 130, for example.

[0071] The server 130 may also provide a cloud service 131 for the data of devices 110, 120, 140, 160. Optionally, further devices may be added, such as peripheral devices for maintaining, providing or processing node 110, 120, 140, 160 data and communication devices for connecting the peripheral devices to the system 100.

[0072] The node 110, 120, 140, 160 may operate as a sensor, such as a biometric sensor.

[0073] The node 110, 120, 140, 160 is capable of locally executing software

program code. The software program code may be a client application of a service whose server application is running on a server 130 of the system 100.

[0074] Embodiments of this invention describe how to implement a system 100 where nodes 110, 120, 140, 160 can store sensitive information in such a way that a remote device later on can confirm the authenticity of the data. The embodiments may use an open distributed ledger to keep a record of hashes of encrypted user data. The data may be encrypted asymmetrically such that anyone can redo the encryption of the raw data. After encryption the data is hashed and the result is added onto a ledger. Additionally a trusted circle 114 for certain nodes can be created and blockchain data divided between the nodes within the trusted circle.

[0075] In an embodiment, a node 110 may be located on the user or on the user household device, on the user's personal smart device, or such, and may continuously collect and encrypt data from the user. The data may include such things a blood pressure, heart rhythm, temperature of household etc. The data may be encrypted asymmetrically, a hash of the asymmetrically encrypted data may be computed by the node and added to a blockchain 170. The blockchain is protected by a proof algorithm, such as proof-of-work, proof-of-stake or the like. The user can now at any time decrypt the data and send it to a third party node 120, 140, 160 (in practice this may be automated, and the user simply chooses which third parties may access which types of data on a continuous basis). The third party 120, 140, 160 can then verify that this was indeed the original data that was collected by the node 110, by first asymmetrically encrypting it, computing the hash and verifying its presence on the blockchain 170.

[0076] The default behavior of the nodes is to not trust other nodes. Hence, the nodes would always store the full blockchain and corresponding data. The owner of the devices can dictate that how the devices utilize shared storage, but nodes cannot have distributed storage outside of the owner's devices. That is to say, if one owner has a couple of nodes and another owner has a couple of nodes, the first owner can make his/her nodes collaborate, but cannot get them to share storage with the second owner's nodes. In some implementations it may be possible for two owners to express mutual consent for their devices to collaborate.

[0077] In an embodiment, a distributed database as disclosed, contains identifiers for certified doctors, people, and certified pharmacies, where doctors issue prescriptions to people using blockchain transactions, and pharmacies provide

medicines to people after receiving prescriptions as transactions from people.

[0078] The procedure in practice, would work like in following steps:

[0079] Step 1) A certified doctor (node 110) creates a prescription (151) and issues transaction that transfers ownership of the prescription to a person (node 120).

[0080] Step 2) The transaction is published in the blockchain 170 if the doctor's certificate allows creation of such transaction.

[0081] Step 3) The person makes a transaction to transfer the prescription (or part of it) to certified pharmacist (node 140).

[0082] Step 4) The transaction is published in the blockchain 170, thus marking the prescription as used.

[0083] Step 5) The person gets the medicine as prescribed.

[0084] In an embodiment, additionally a fourth party (node 140) may be introduced, which could be a government. This fourth party could be used to ensure doctor is not issuing too much medicine or that the medicine is not in conflict with something (e.g. with other medicine some other doctor has prescribed for the person, or if too high dosage is prescribed), for example.

[0085] In that case, the procedure in practice would in that case (new step 3) be:

[0086] Step 1) A certified doctor (node 110) creates a prescription 151 and issues transaction that transfers ownership of the prescription to a person (node 120).

[0087] Step 2) The transaction is published in the blockchain 170 if the doctor's certificate allows creation of such transaction.

[0088] Step 3) The transaction is signed by a government entity, or like (node 140) that approves the prescription 151, and then published again the blockchain 170.

[0089] Step 4) The person makes a transaction to transfer the prescription (or part of it) to certified pharmacist (node 160).

[0090] Step 5) The transaction is published in the blockchain 170, thus marking the prescription as used.

[0091] Step 6) The person gets the medicine.

[0092] One difference to other asset tracking ideas is that in this case the asset can only be used for two transactions and only between different types of owners. That is new transaction can only be created by doctor (or alike), it can be transferred

only once to a person, and the person can transfer it only once to pharmacist, after which the transaction is in terminal state, for example.

[0093] In an embodiment, for partially consumed prescription the pharmacy (third user/node 160) can modify the prescription (e.g. subtracts the amount of medicine given to patient from prescription) and transacts it back to patient (second user/node 120).

[0094] In an embodiment, for fully consumed prescription the pharmacy (third user/node 160) can, for example, transact the prescription back to the patient (second user/node 120), transact the prescription back to the doctor (first user/node 110), transact the prescription back to the administrator (fourth user/node 140), or terminate the prescription (not transact anywhere).

[0095] Fig. 2 shows another schematic drawing of a system 200 of an example embodiment.

[0096] A system comprises a plurality of nodes. The data may be divided between the nodes in various ways. The data may comprise blockchain and corresponding transaction data.

[0097] In an embodiment, a distributed ledger can be considered a general database where each table may implement, for example, the ability to add, remove or modify records. In the example implementation of Fig. 2, every request to modify the database may be collected into a Merkle tree 230 (In Fig. 2 there are two Merkle trees) that is then used to generate a blockchain 170.

[0098] In an embodiment, transactions may be chained directly, leaving out the Merkle tree(s). This may be the preferred in certain circumstances. The order in which events occur is typically agreed upon using a consensus mechanism, such as proof-of-work, proof-of-stake, majority voting or preselected validation nodes.

[0099] In an embodiment, a prescription issued by a doctor, is discussed.

[00100] Prescriptions are typically issued by doctors. By consensus transactions by any personal that is not a certified doctor is rejected as an invalid transaction. In one embodiment, it is enough for the doctor to know the patients public key to issue the prescription.

[00101] In an embodiment, following steps may be carried out:

[00102] Step 1) A doctor writes a prescription.

[00103] Step 2) The new prescription is placed on a file system, where there is shared access between pharmacies and doctors.

[00104] Step 3) A transaction is created containing the patient's id, the hash of the prescription, a pointer to where the file is located and the doctor's public key.

[00105] Step 4) The transaction is signed by the doctor (e.g. doctor's private key).

[00106] Step 5) The signed transaction is distributed on the network.

[00107] In an embodiment, a prescription delivered by a pharmacist, is illustrated.

[00108] At the pharmacist, the patient presents his/her ID to the pharmacists and, in an example embodiment, the prescription is fulfilled as follows:

[00109] Step 1) The pharmacist presents the patient with a challenge to verify his/her identity. In an embodiment, the patient signs the previous record issued by the doctor thus verifying their identity.

[00110] Step 2) The signed prescription is verified against a set of rules determined by the local legislature.

[00111] Step 3) The pharmacist creates a transaction that invalidates the prescription.

[00112] Step 4) The transaction is signed by the pharmacist and the patient.

[00113] Step 5) The transaction is verified and added to the next block according to the consensus algorithm.

[00114] Step 6) The pharmacist hands over the medications to the patient.

[00115] In an embodiment as shown in Fig. 2, a blockchain 170 is used to establish a public record 240, 250 of certified doctors, certified pharmacies, prescriptions and optionally health records. To store health records and prescriptions, the system may implement a massively replicated distributed file system. In an example implementation, the ledger contains at least one table that keeps track of certified doctors 240 and another keeping track of certified pharmacists. Additionally, it contains a ledger that has at least a hash entry, a pointer to a file, a doctor's ID and patient ID. The hash entry is the hash of a file on a file system accessible to both the doctors and pharmacist. The IDs are used to represent actors in the system, such as doctors, pharmacists and patients. In the preferred implementation the IDs are public keys, each of which has a corresponding private key. The person in possession of the private key is the sole owner of the ID, thus making them the only person capable of signing transactions involving that ID.

[00116] In an embodiment, a variant of majority voting that is preferred due to its low deployment cost, may be utilized.

[00117] In an embodiment, a block 210 is processed by combining previous block information (e.g., a hash of a block header) from blockchain 170 with additional information, thereby linking the block 210 with the blockchain 170. The additional transaction information can include time stamp, prescription related data, a digital signature, and a token, for example. A peer node can re-calculate a value for the block, typically a hash of the block's header along with hash information from the transactions, until the resulting value satisfies the validity requirement. For example, in embodiments where block 210 is processed via a hash function (e.g., SHA256, Script, etc.), peer can increment a nonce value until a hash is generated having the desired proof-of-work characteristics, perhaps a number of leading zero bits among other factors, for example.

[00118] Once validity block 210 has been properly calculated and/or validated by the peers, it can be sent to other peers in the system so that the validity block 210 will be appended to the blockchain 170. Thus, validity block 210 becomes part of the chronicled healthcare prescription history of stakeholder, such as a patient. Validity block 210 can be considered accepted as part of the blockchain 170 once other peers pickup and integrate it into their own copies of the blockchain 170.

[00119] In an embodiment, a previous block 210 and a current block 220 are illustrated in Fig. 2, and illustrating how combined hash of the previous block 210 is used for generation of current block 220 in the blockchain 170.

[00120] In an embodiment, different uses of public-key cryptography may be utilized. To ensure confidentiality, public-key encryption may be used, in which a message is encrypted with a recipient's public key. The message cannot be decrypted by anyone who does not possess the matching private key, who is thus presumed to be the owner of that key and the person associated with the public key.

[00121] To ensure tamper-proof, digital signatures (signing) may be utilized, in which a message is signed with the sender's private key and can be verified by anyone who has access to the sender's public key. This verification proves that the sender had access to the private key, and therefore is likely to be the person associated with the public key. This also ensures that the message has not been tampered with, as any manipulation of the message will result in changes to the encoded message digest, which otherwise remains unchanged between the sender and receiver.

[00122] Fig. 2 further illustrates a transaction record 240 for adding a certified

doctor to the distributed file system, a transaction record 250 for removing a certified doctor from the distributed file system, and a transaction record 260 for adding a certified device to the distributed file system.

[00123] At the time where a proof-of-work (POW) should be found, the nodes may combine the hashes from the transactions to form a Merkle tree 230, or simply keep a hash of the state of the full storage system, which will enter the next block. In some implementations it may be feasible to do both as this allows to implement a fast-forward mechanism that makes new nodes catch up with the network in much less time than what they would need if only the Merkle hash of the transactions are stored in the blocks.

[00124] In addition to distributing the storage, the nodes may also distribute hash power. This may happen within a trusted circle and it may be done across subsets of the networks by making pools, for example. Unlike the storage, distribution of the hash power does not require trust and can therefore easily be implemented in many various scenarios.

[00125] In an embodiment, transaction data may be generated by a first node, such as a doctor node. The transaction data is hashed using a cryptographic hashing function, to create a cryptographic hash block, the cryptographic hash block is associated with a digital signature of the doctor node and may be transmitted to a public block chain.

[00126] In an embodiment, a node identifier is assigned to each node, wherein the node identifier may comprise a public key.

[00127] Furthermore, a trusted user circle identifier may be assigned to the trusted user circle. Routing transactions from nodes external to the trusted user circle may base on the trusted user circle identifier.

[00128] The transaction data, such as a prescription data item, may be stored at a node that adds a hash of an asymmetric encryption on to generate a hash block 210, 220. In some embodiments, the data may be stored directly on the node.

[00129] The hash block 210, 220 of the asymmetrically encrypted data may be computed and added to a block chain 170. The block chain 170 may be protected by a proof algorithm, such as proof-of-work (POW), proof-of-stake or the like. The user can now at any time decrypt the data and send it to a third party within a network system 100, 200 (in practice this may be automated, and the user simply chooses which third parties may access which types of data on a continuous basis). The third

party can then verify that this was indeed the original data that was collected by the node, by first asymmetrically encrypting it, computing the hash and verifying its presence in the block chain 170. Nodes may be nodes in a network of nodes, such as a network for Internet of Things (IoT).

[00130] In an embodiment, the block chain 170 is implemented using Merkle trees 230. Aggregating hash values of the exchanged data in a Merkle tree 230 is efficient, since the "root" 210, 220 of the Merkle tree 230 provides a compressed digest of all individual hash values, so that the Merkle tree 230 reduces storage requirements.

[00131] A distributed ledger is a database that can securely record user transaction data for sharing across a network through entirely transparent updates of information.

[00132] The block chain data structure 170 is an ordered, back-linked list of blocks of transactions. The blockchain 170 can be stored as a flat file, or in a simple database. Blocks 210, 220 are linked "back" each referring to the previous block in the chain. The blockchain 170 is often visualized as a vertical stack, with blocks layered on top of each other and the first block serving as the foundation of the stack. The visualization of blocks stacked on top of each other results in the use of terms such as "height" to refer to the distance from the first block, and "top" or "tip" to refer to the most recently added block.

[00133] Although a block has just one parent, it can temporarily have multiple children. Each of the children refers to the same block as its parent and contains the same (parent) hash in the "previous block hash" field. Eventually, only one child block becomes part of the blockchain 170. Even though a block may have more than one child, each block 210, 220 can have only one parent. This is because a block has one single "previous block hash" field referencing its single parent.

[00134] Each block within the blockchain 170 may be identified by a hash, generated e.g. using a SHA256 cryptographic hash algorithm on the header of the block. Each block also references a previous block, known as the parent block, through the "previous block hash" field in the block header. In other words, each block contains the hash of its parent inside its own header. The sequence of hashes linking each block to its parent creates a chain going back all the way to the first block ever created, known as the genesis block.

[00135] In an embodiment, each block in the block chain 170 contains a summary of all the transactions in the block, using a Merkle tree 230. The Merkle tree 230,

also known as a binary hash tree, is a data structure used for efficiently summarizing and verifying the integrity of large sets of data. Merkle trees are binary trees containing cryptographic hashes. The term "tree" is used in computer science to describe a branching data structure, but these trees are usually displayed upside down with the "root" at the top and the "leaves" at the bottom of a diagram.

[00136] In an embodiment, the Merkle tree is omitted and blocks of "transactions" are linked directly together in the private block chain 170.

[00137] The digital block chain 170 corresponds to a distributed cryptographic ledger shared amongst certified and trusted nodes, over which every successfully performed transaction is recorded.

[00138] In an embodiment, a private block chain of a trusted circle may be integrated to a public block chain.

[00139] In an embodiment, received transaction data from a first node (e.g. doctor) at a remote device (e.g. patient) can be verified by the remote device. The remote device may be a computer, a smart device, a server, an embedded device or special purpose circuit, for example.

[00140] In an embodiment, one may want to store the data unencrypted in which case the asymmetric encryption can be omitted in both cases. In some embodiments the transaction data may be encrypted and hashed by the node itself and only accepted onto the ledger 230, if a node public key is verified as a certified device.

[00141] In an embodiment, each device, including IoT (Internet of Things) devices, or node, may comprise a private key for asymmetric cryptography. The asymmetric cryptographic system uses pairs of keys: public keys that may be disseminated widely paired with private keys, which are known only to the owner. There are two functions that can be achieved: using a public key to authenticate that a prescription or message originated with a holder of the paired private key; or encrypting a message or prescription data item with a public key to ensure that only the holder of the paired private key can decrypt it.

[00142] The private key may be configured to the node by the manufacturer or reseller of the node. Then, when joining e.g. a trusted circle, the node may update its public key to a gateway node of the trusted circle. Alternatively, a node may receive a private key from the gateway node when joining the trusted circle and the corresponding public key made available by the gateway node.

[00143] In an embodiment, a patient or pharmacist node device 120, 140 (Fig. 1)

receives transaction data from a doctor node device 110. The patient or pharmacist device 120, 140 hashes the transaction data using a cryptographic hashing function, to create a cryptographic hash block and fetches a reference cryptographic hash block from block chain 170. The device 120, 140 may then compare the cryptographic hash block to the fetched block from the block chain 170. The transaction data may be verified in response to finding a matching cryptographic hash block in a block chain 170 based on the comparing step.

[00144] Various embodiment of the invention disclosed in the following relate to electronic circuits used in IoT. Furthermore, IoT may be implementing biomedical measurements. Herein, the term biomedical measurement is generally used to refer to electronic measurement of biomedical substance or organic material. The biomedical substance may be for example body or tissue of a living organism (e.g. human being) or a cell sample. Examples of biomedical measurements comprise for example electrocardiography (ECG) measurements, electrodermal activity (EDA, aka GSR galvanic skin response) measurements, body conductivity (aka bioimpedance) measurements, and impedance plethysmography (IPG) measurements, e.g. impedance cardiography (ICG).

[00145] In an embodiment, government majority consensus may be provided. Thus, an additional record keeping track of official government nodes may be present in the system 200. The genesis block is minted with one or more governments public keys registered into this block. Upon reaching the end of a block period, everyone who holds a government private key votes about which block is the next valid block. This effectively solves the high energy consumption with proof-of-work (POW, but yet remains secure as multiple nodes across a large geographical area makes it hard to make a single attack.

[00146] New government keys can be added or removed by majority voting, where each vote is cast by signing a transaction for, or against adding a new government role. In this manner, the network can be expanded. This allows deployment to start with one country, and addition of countries later on.

[00147] In an embodiment, different certification schemes can be used in order to establish certificates for doctors and pharmacies, for example.

[00148] In one scheme, government keys are directly used to certify doctors and pharmacies. However, given that the number of doctors is rather large and that the number of government keys is expected to be low, this may become inefficient and

cumbersome. Instead, one may add an additional certification record onto the ledger registering “clinics” or regional authorities. These local authorities are then given the right to certify doctors and pharmacies. In principle, this hierarchy can be arbitrarily deep, but in practice is good to limit the depth as much as possible for security and bureaucracy reasons. Trusted circles may be utilized, for example.

[00149] In the lack of authority roles on the system, an alternative method to certify doctors and pharmacies is by plain majority voting. While this could work for small local communities, it is possible to break down if scaled up. In addition, this method would have to rely on proof-of-work (POW) as the system in nature is entirely untrusted.

[00150] In an embodiment, reoccurring prescriptions may be utilized. It may also include the ability to authorize a person to pick up a prescription on behalf of the patient of the actual prescription.

[00151] In an embodiment, it is possible to have different degrees of authorization for different types of healthcare professionals. This may involve granting limited prescription and/or fulfillment rights to trainee doctors, nurses and pharmacists. These details are allowed to vary from country to country. For example, country A may permit a clinical pharmacist to create prescriptions for a certain type of medicine, while country B only allows full doctors to create such prescriptions.

[00152] Any extra authorization required by the local legislature can be included in the prescriptions. An example of this might be to require a doctor to sign off on a prescription created by a nurse before it is valid. Similarly, a trainee pharmacist may not be able to fulfill prescriptions for certain types of medications, for example.

[00153] Fig. 3 shows a flow diagram illustrating a method for blockchain verification of healthcare prescriptions. In step 310, the method is started. In step 320, a prescription data item is generated by a first user authorized to generate the prescription data item. In step 330, the prescription data item is associated to a first transaction. In step 340, the first transaction is recorded to a blockchain, the first transaction transferring ownership of the prescription data item to a second user. In step 350, a second transaction is recorded to the blockchain, the second transaction transferring ownership of at least part of the prescription data item to a third user. In step 360, the prescription data item is modified by the third user. In step 370, a third transaction is recorded to the blockchain, the third transaction transferring ownership of the modified prescription data item to the second user. The method ends at step

380.

[00154] Fig. 4 presents an example block diagram of a node of device or apparatus 110, 120, 140, 160 in which various embodiments of the invention may be applied. The device or apparatus 110, 120, 140, 160 may be a sensor device, a smart device, a computer device, a user device, a user wearable device or a hub device. All elements described in Fig. 4 are not necessary to be implemented in the same device.

[00155] In an embodiment, a sensor 470 may be implemented as a separate device (e.g. a user wearable device) communicating via the communication interface 450 with other device, or as an integrated sensor 460 within the device. The user interface 440 may be implemented also in another device connected via a communication interface 450 to the device 110, 120, 140, 160. Such device may comprise a mobile phone, a smart phone, or a tablet, for example. In an embodiment, the device 110, 120, 140, 160 may communicate with a plurality of sensors 460, 470, both internal and external sensors, and of a plurality of users.

[00156] The general structure of the device 110, 120, 140, 160 comprises a user interface 440, a communication interface 450, a processor 410, and a memory 420 coupled to the processor 410. The device 110, 120, 160, 170 further comprises software 430 stored in the memory 420 and operable to be loaded into and executed in the processor 410. The software 430 may comprise one or more software modules and can be in the form of a computer program product. Not all elements of Fig. 4 are necessary but optional for the device 110, 120, 140, 160 such as the user interface 440 and sensors 460, 470.

[00157] The processor 410 may be, e.g., a central processing unit (CPU), a microprocessor, a digital signal processor (DSP), a graphics processing unit, or the like. Fig. 4 shows one processor 410, but the device 110, 120, 140, 160 may comprise a plurality of processors.

[00158] The memory 420 may be for example a non-volatile or a volatile memory, such as a read-only memory (ROM), a programmable read-only memory (PROM), erasable programmable read-only memory (EPROM), a random-access memory (RAM), a flash memory, a data disk, an optical storage, a magnetic storage, a smart card, or the like. The device 110, 120, 140, 160 may comprise a plurality of memories. The memory 420 may be constructed as a part of the device 110, 120, 140, 160 or it may be inserted into a slot, port, or the like of the device 110, 120, 140,

160 by a user. The memory 420 may serve the sole purpose of storing data, or it may be constructed as a part of an apparatus serving other purposes, such as processing data.

[00159] The user interface 440 may comprise circuitry for receiving input from a user of the device 110, 120, 140, 160, e.g., via a keyboard, a touchpad, a motion sensor, a touch-screen of the device 110, 120, 140, 160 speech recognition circuitry, gesture recognition circuitry or an accessory device, such as a headset or a remote controller, for example. Furthermore, the user interface 440 may comprise circuitry for providing output for the user via a display, a speaker, a touch-sensitive display or a tactile feedback device, for example.

[00160] The communication interface module 450 implements at least part of data transmission. The communication interface module 450 may comprise, e.g., a wireless or a wired interface module. The wireless interface may comprise such as a WLAN, Bluetooth, infrared (IR), radio frequency identification (RF ID), NFC, GSM/GPRS, CDMA, WCDMA, or LTE (Long Term Evolution) radio module. The wired interface may comprise such as universal serial bus (USB), HDMI, SCART or RCA, for example. The communication interface module 450 may be integrated into the device 110, 120, 140, 160 or into an adapter, card or the like that may be inserted into a suitable slot or port of the device 110, 120, 140, 160. The communication interface module 450 may support one radio interface technology or a plurality of technologies. The communication interface module 450 may support one wired interface technology or a plurality of technologies. The device 110, 120, 140, 160 may comprise a plurality of communication interface modules 450.

[00161] In an embodiment, the communication interface module 450 may comprise location modules for tracking location of the device 110, 120, 140, 160. Such location modules may comprise a module for satellite based global positioning system (e.g. GPS), a module for cellular based positioning system, a module for wireless non-cellular positioning system (e.g. Wi-Fi) or a module for hybrid positioning system, for example.

[00162] A skilled person appreciates that in addition to the elements shown in Fig. 4, the device 110, 120, 140, 160 may comprise other elements, such as microphones, speakers, sensors, cameras, as well as additional circuitry such as input/output (I/O) circuitry, memory chips, application-specific integrated circuits (ASIC), processing circuitry for specific purposes such as source coding/decoding

circuitry, channel coding/decoding circuitry, ciphering/deciphering circuitry, and the like. Additionally, the device 110, 120, 140, 160 may comprise a disposable or rechargeable battery (not shown) for powering when external power if external power supply is not available.

[00163] In an embodiment, the device 110, 120, 140, 160 comprises an additional sensor 460, 470 for providing metadata associated to the transaction data (e.g. biometric information). The metadata may comprise at least one of the following: temperature information; pressure information; fingerprint information; retinal scan information; movement information; location information; and humidity information.

[00164] In an embodiment, the device 110, 120, 140, 160 comprises speech or gesture recognition means. Using these means, a pre-defined phrase or a gesture may be recognized from the speech or the gesture and translated into control information for the device 110, 120, 140, 160.

[00165] In an embodiment, a device 140 may correspond to the block structure of Fig. 4 without sensors 460, 470, for example.

[00166] User wearable devices and sensors thereof provided in various embodiments may be used for example in heart rate detection, blood pressure detection, lactate level detection, respiration, impedance cardiography (ICG), bioelectrical impedance analysis (BIA), fingerprint detection, retinal scan detection, electrical impedance tomography (EIT) and electrodermal activity (EDA, aka GSR galvanic skin response) measurements, for example.

[00167] Fig. 5 shows a block diagram of a server apparatus 130 of an example embodiment. The general structure of the server apparatus 130 comprises a processor 510, and a memory 520 coupled to the processor 510. The server apparatus 130 further comprises software 530 stored in the memory 520 and operable to be loaded into and executed in the processor 510. The software 530 may comprise one or more software modules and can be in the form of a computer program product.

[00168] The processor 510 may be, e.g., a central processing unit (CPU), a microprocessor, a digital signal processor (DSP), a graphics processing unit, or the like. Fig. 5 shows one processor 510, but the server apparatus 130 may comprise a plurality of processors.

[00169] The memory 520 may be for example a non-volatile or a volatile memory, such as a read-only memory (ROM), a programmable read-only memory (PROM),

erasable programmable read-only memory (EPROM), a random-access memory (RAM), a flash memory, a data disk, an optical storage, a magnetic storage, a smart card, or the like. The server apparatus 130 may comprise a plurality of memories. The memory 520 may be constructed as a part of the server apparatus 130 or it may be inserted into a slot, port, or the like of the server apparatus 130 by a user. The memory 520 may serve the sole purpose of storing data, or it may be constructed as a part of an apparatus serving other purposes, such as processing data.

[00170] The communication interface module 550 implements at least part of data transmission. The communication interface module 550 may comprise, e.g., a wireless or a wired interface module. The wireless interface may comprise such as a WLAN, Bluetooth, infrared (IR), radio frequency identification (RF ID), GSM/GPRS, CDMA, WCDMA, or LTE (Long Term Evolution) radio module. The wired interface may comprise such as Ethernet or universal serial bus (USB), for example. The communication interface module 550 may be integrated into the server apparatus 130, or into an adapter, card or the like that may be inserted into a suitable slot or port of the server apparatus 130. The communication interface module 550 may support one radio interface technology or a plurality of technologies. Configuration information between the nodes 110, 120, 140, 160 and the system server 130 may be transceived using the communication interface 550. Similarly, account creation information between the system server 130 and a service provider may be transceived using the communication interface 550.

[00171] An application server 540 provides application services e.g. relating to the user accounts stored in a user database 570 and to the service information stored in a service database 560. The service information may comprise content information, content management information or metrics information, for example. The service information may also comprise information relating to transaction data, prescription data, history data of earlier transaction data, or blockchains, for example.

[00172] A skilled person appreciates that in addition to the elements shown in Fig. 5, the server apparatus 130 may comprise other elements, such as microphones, displays, as well as additional circuitry such as input/output (I/O) circuitry, memory chips, application-specific integrated circuits (ASIC), processing circuitry for specific purposes such as source coding/decoding circuitry, channel coding/decoding circuitry, ciphering/deciphering circuitry, and the like.

[00173] In an embodiment, in case of a trusted circle, a trusted circle may be

initially setup by any trusted node within the system according to pre-defined settings. Hashing and encrypting may be balanced for nodes having better processing power, security, memory capacity and/or powering. Hashing and encryption may also be user changeable based on the user settings or based on the local system administrator, for example.

[00174] Without in any way limiting the scope, interpretation, or application of the claims appearing below, a technical effect of one or more of the example embodiments disclosed herein is that an improved construction and storage of transaction data of blockchain is provided that allows prescription data item secure processing in a blockchain network.

[00175] Another technical effect of one or more of the example embodiments disclosed herein is that security of sensitive transaction data transmission between different devices and stakeholders is improved. Another technical effect of one or more of the example embodiments disclosed herein is that reliability of prescription transaction data, relating to a plurality of nodes, is improved.

[00176] Another technical effect of one or more of the example embodiments disclosed herein is that less complex systems and nodes are required for prescription data item ordering, collecting and verification.

[00177] Without in any way limiting the scope, interpretation, or application of the claims appearing below, a technical effect of one or more of the example embodiments disclosed herein is that an improved transaction data service system is provided.

[00178] If desired, the different functions discussed herein may be performed in a different order and/or concurrently with each other. Furthermore, if desired, one or more of the before-described functions may be optional or may be combined.

[00179] Although various aspects of the invention are set out in the independent claims, other aspects of the invention comprise other combinations of features from the described embodiments and/or the dependent claims with the features of the independent claims, and not solely the combinations explicitly set out in the claims.

[00180] It is also noted herein that while the foregoing describes example embodiments of the invention, these descriptions should not be viewed in a limiting sense. Rather, there are several variations and modifications, which may be made without departing from the scope of the present invention as defined in the appended claims.

CLAIMS

1. A computer-implemented method for blockchain verification of healthcare prescriptions, the method comprising:

5 generating a prescription data item by a first user authorized to generate the prescription data item;

 associating the prescription data item to a first transaction;

 recording the first transaction to a blockchain, the first transaction transferring ownership of the prescription data item to a second user;

10 recording a second transaction to the blockchain, the second transaction transferring ownership of at least part of the prescription data item to a third user;

 modifying the prescription data item by the third user; and

 recording a third transaction to the blockchain, the third transaction transferring ownership of the modified prescription data item to the first user, the second user or
15 a fourth user.

2. The method of claim 1, further comprising:

 signing the prescription data item by a fourth user in response to recording the first transaction to the blockchain; and

20 recording the second transaction to the blockchain in response to signing the prescription data item by the fourth user.

3. The method of claim 1 or 2, wherein

 the first user being a doctor prescribing the prescription data item;

25 the second user being a patient the prescription data item being prescribed for;

 the third user being a certified pharmacist; and

 the fourth user being an administrator.

4. The method of claim 3, further comprising:

30 determining received prescription information by the third user, the received prescription information corresponding to medicines received by the second user; and

 modifying the prescription data item by the third user based on the received prescription information.

5. The method of any of claims 1 to 4, further comprising:
defining a blockchain record comprising certified first users.
- 5 6. The method of any of claims 1 to 5, further comprising:
defining a blockchain record comprising certified third users.
7. The method of any of claims 1 to 6, further comprising:
defining a blockchain record comprising certified fourth users.
- 10 8. The method of any of claims 1 to 7, wherein the first transaction comprising:
an identifier of the second user;
a hash value of the prescription data item; and
a public key of the first user.
- 15 9. The method of claim 8, further comprising:
signing the prescription data item by the first user; and
recording the signed prescription data item as a transaction to the blockchain in
response to signing the prescription data item by the first user.
- 20 10. The method of any of claims 1 to 9, further comprising:
receiving, by the second user, a challenge from the third user to verify an
identity of the second user.
- 25 11. The method of claim 10, further comprising:
signing, by the second user, a previous blockchain record issued by the first
user to verify identity of the second user.
12. The method of any of claims 1 to 11, further comprising:
30 generating a third transaction, by the third user, to invalidate at least part of the
prescription data item.
13. The method of claim 12, further comprising:
signing the third transaction by the third user and the second user.

14. The method of claim 13, wherein at least one of the first, second or third transaction is added as a next block to the blockchain according to a consensus algorithm.

5

15. The method of any of claims 1 to 14, further comprising:

receiving a certificate of a first user;

verifying that the certificate being authorized for generating the prescription data item; and

10

in response to successful authorization, recording the first transaction to the blockchain, the first transaction transferring ownership of the prescription data item to the second user.

16. The method of any of claims 1 to 15, further comprising:

15

assigning a node identifier to each node of the first, the second and the third user.

17. The method of claim 16, wherein the node identifier comprising a public key.

20

18. The method of claim 16 or 17, wherein the first, the second and the third user are connected to a wide area communication interface.

19. The method of any of claims 1 to 18, wherein the blockchain is configured to be protected by a proof algorithm comprising at least one of a proof-of-work, proof-of-stake and majority-voting algorithm.

25

20. An apparatus comprising:

a communication interface for transceiving information;

at least one processor; and

30

at least one memory including computer program code;

the at least one memory and the computer program code configured to, with the at least one processor, cause the device to:

generate a prescription data item by a first user authorized to generate the prescription data item;

associate the prescription data item to a first transaction;

record the first transaction to a blockchain, the first transaction transferring ownership of the prescription data item to a second user;

5 record a second transaction to the blockchain, the second transaction transferring ownership of at least part of the prescription data item to a third user;

modify the prescription data item by the third user; and

10 record a third transaction to the blockchain, the third transaction transferring ownership of the modified prescription data item to the first user, the second user or a fourth user.

21. The apparatus of claim 20 comprising a plurality of user devices operated by at least two of the first user, the second user, the third user and the fourth user.

15 22. A computer program embodied on a computer readable non-transitory medium comprising computer executable program code, which when executed by at least one processor of a apparatus, causes the apparatus to:

generate a prescription data item by a first user authorized to generate the prescription data item;

20 associate the prescription data item to a first transaction;

record the first transaction to a blockchain, the first transaction transferring ownership of the prescription data item to a second user;

record a second transaction to the blockchain, the second transaction transferring ownership of at least part of the prescription data item to a third user;

25 modify the prescription data item by the third user; and

record a third transaction to the blockchain, the third transaction transferring ownership of the modified prescription data item to the first user, the second user or a fourth user.

30

1 / 4

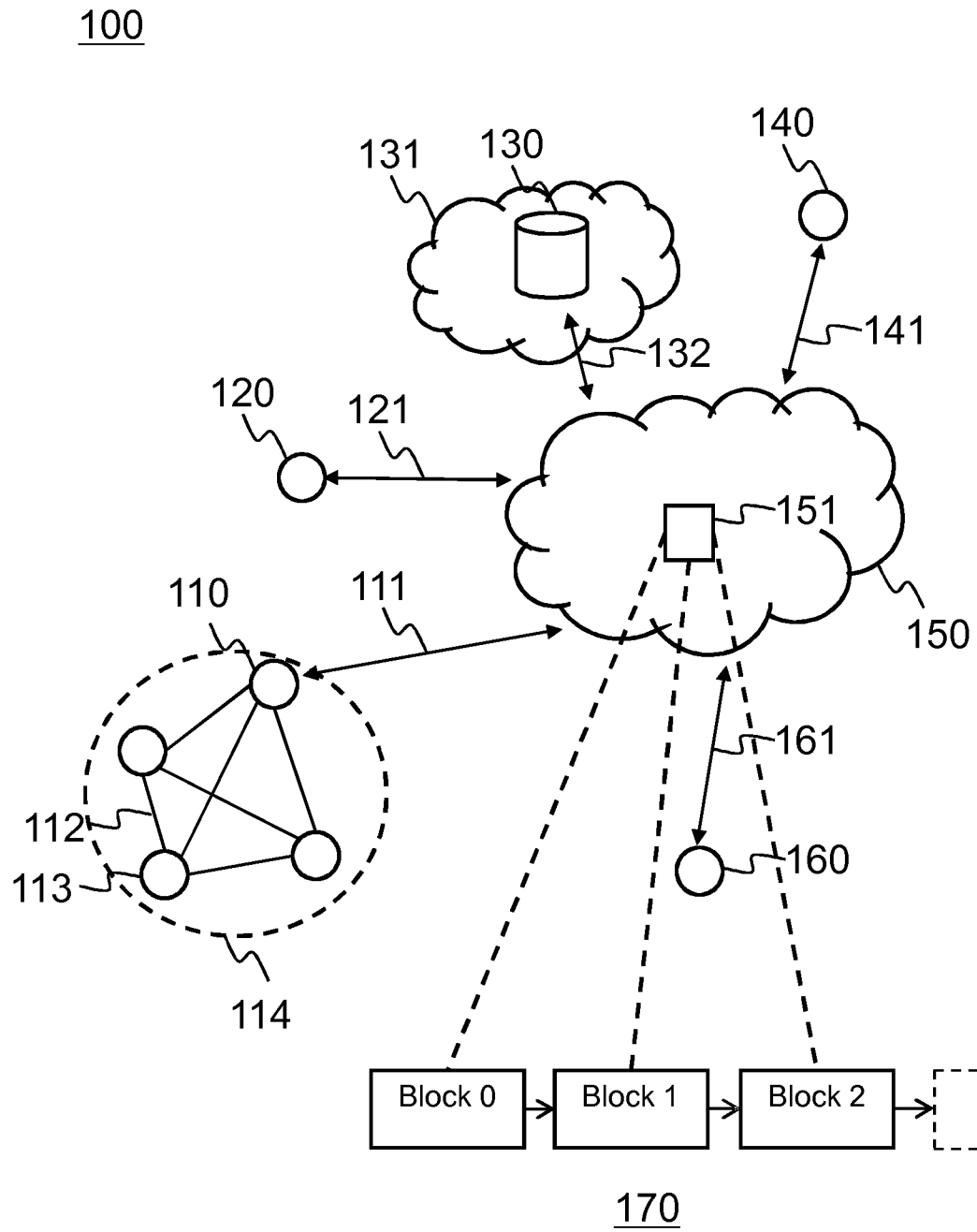


Fig. 1

2 / 4

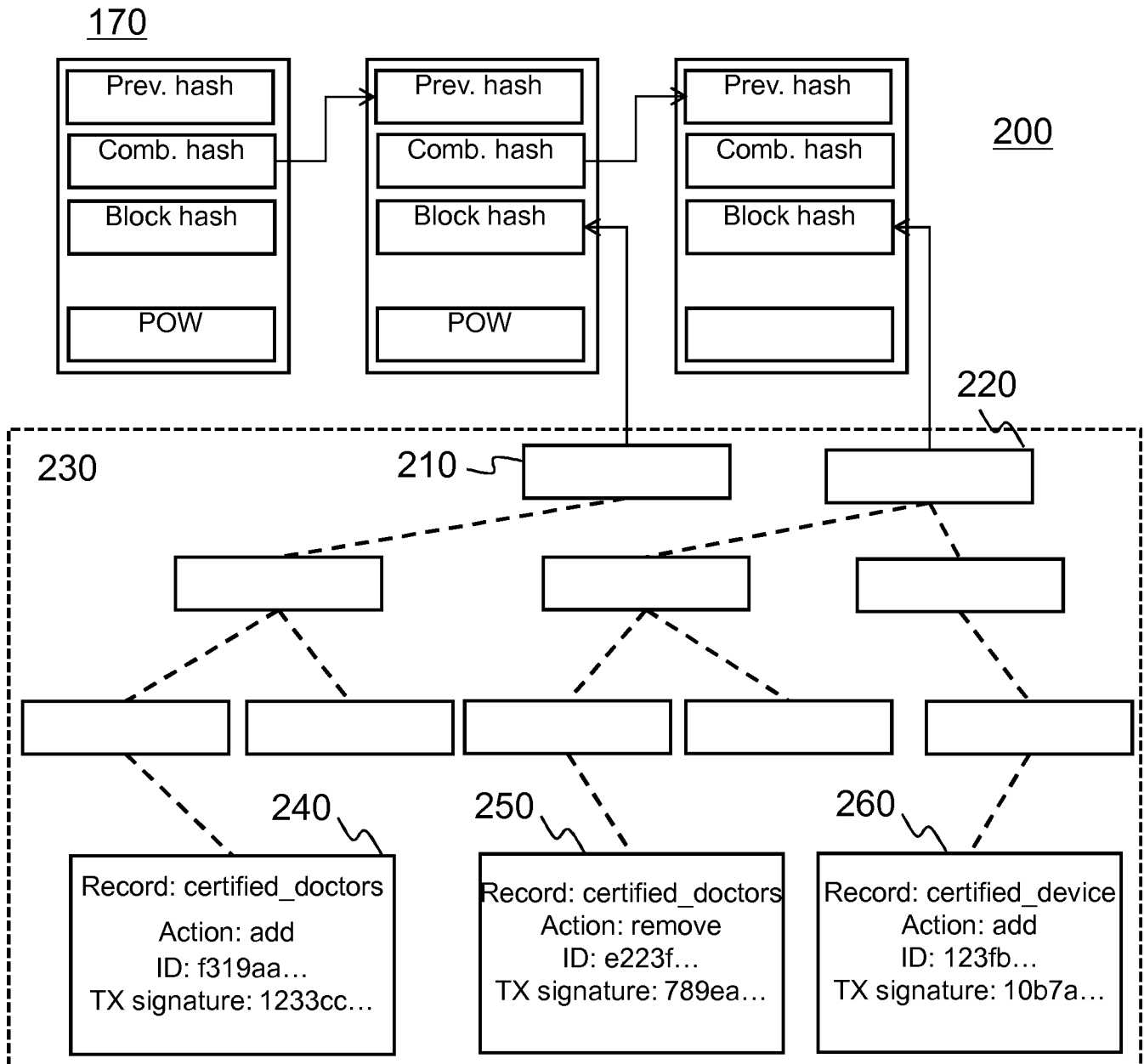


Fig. 2

3 / 4

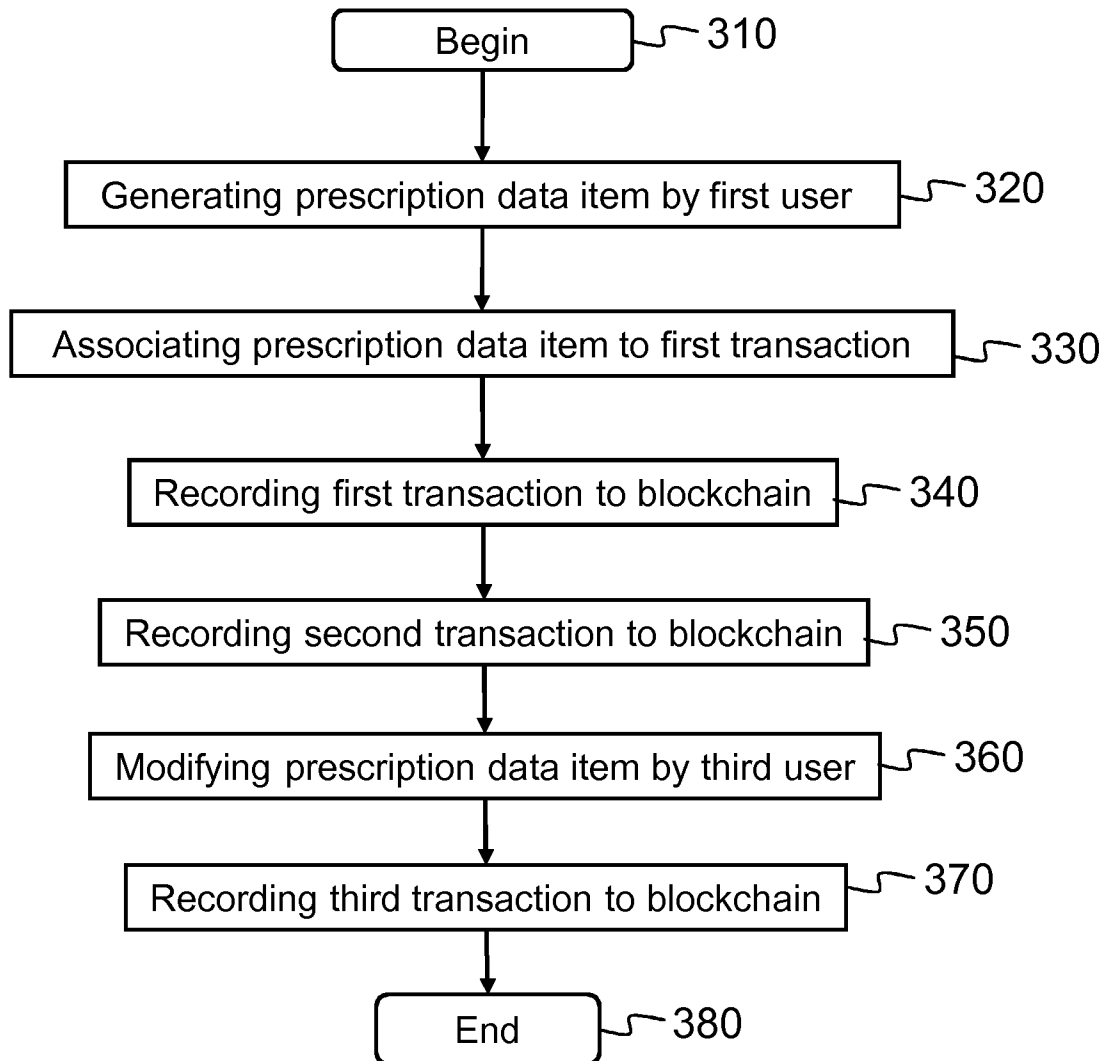


Fig. 3

4 / 4

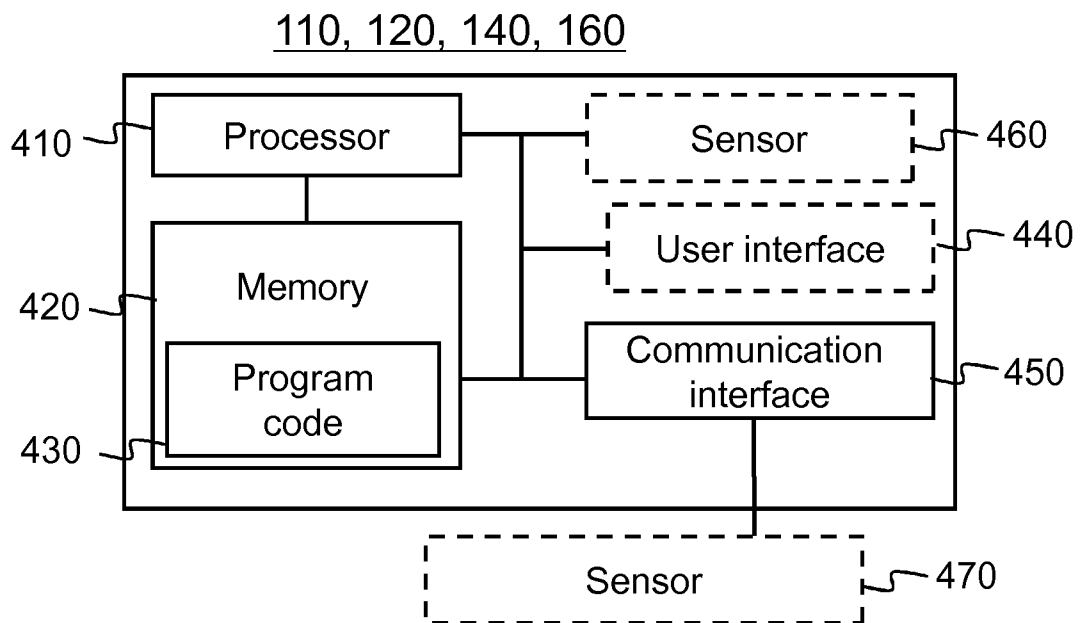


Fig. 4

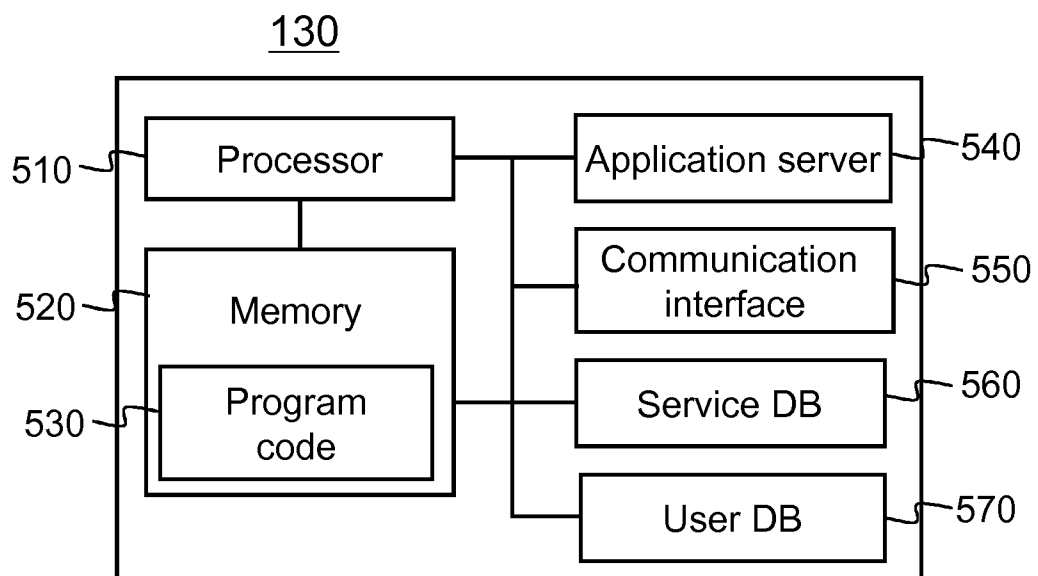


Fig. 5

INTERNATIONAL SEARCH REPORT

International application No
PCT/FI2016/050572

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q50/22
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06Q

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

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

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Melanie Swan: "Blockchain: Blueprint for a New Economy", 8 February 2015 (2015-02-08), O'Reilly, XP055279098, ISBN: 978-1-4919-2049-7 page vii - page xii page 59 - page 61 -----	1-22
X	Pedro Franco: "Understanding Bitcoin: Cryptography, Engineering and Economics", 24 November 2014 (2014-11-24), Wiley, XP055279012, ISBN: 978-1-119-01916-9 pages ToC, Ch01-Ch04, page 8 - page 10 page 15 - page 16 ----- -/--	1-22



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

4 October 2016

Date of mailing of the international search report

13/10/2016

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Krafft, Gerald

INTERNATIONAL SEARCH REPORT

International application No

PCT/FI2016/050572

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	William Mougayar: "The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology", 9 May 2016 (2016-05-09), Wiley, XP055306781, ISBN: 978-1-119-30031-1 page Ch05, Chapter 5 -----	1-22
X	Siraj Raval: "Decentralized Applications: Harnessing Bitcoin's Blockchain Technology", 8 August 2016 (2016-08-08), O'Reilly, XP055306925, ISBN: 978-1-4919-2454-9 page 6 - pages 7,11,15 -----	1-22
X	Andreas M. Antonopoulos: "Mastering Bitcoin - Unlocking Digital Cryptocurrencies", 20 December 2014 (2014-12-20), O'Reilly Media, Beijing Cambridge Farnham Köln Sebastopol Tokyo, XP055306939, ISBN: 978-1-4493-7404-4 page 228 - page 231 -----	1-22
X	Wikipedia: "Blockchain (database)", INTERNET ARTICLE, 20 August 2016 (2016-08-20), XP055306814, Retrieved from the Internet: URL:https://en.wikipedia.org/w/index.php?title=Blockchain_(database)&oldid=735327455 [retrieved on 2016-09-30] the whole document -----	1-22
X	SIMON BARBER ET AL: "Bitter to Better How to Make Bitcoin a Better Currency", 2 March 2012 (2012-03-02), FINANCIAL CRYPTOGRAPHY AND DATA SECURITY, SPRINGER BERLIN HEIDELBERG, BERLIN, HEIDELBERG, PAGE(S) 399 - 414, XP047013846, ISBN: 978-3-642-32945-6 the whole document -----	1-22
A	US 2015/230761 A1 (BRUMBACK CHRISTINE BOOMER [US] ET AL) 20 August 2015 (2015-08-20) the whole document -----	1-22

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/FI2016/050572

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2015230761 A1	20-08-2015	US 2014142403 A1	22-05-2014
		US 2014378787 A1	25-12-2014
		US 2015230761 A1	20-08-2015
