



(51) International Patent Classification:

G06F 17/30 (2006.01) G06Q 20/38 (2012.01)
G06F 3/06 (2006.01) G06Q 20/06 (2012.01)
G06Q 20/22 (2012.01) G06Q 50/24 (2012.01)

(21) International Application Number:

PCT/FI2016/050841

(22) International Filing Date:

30 November 2016 (30.11.2016)

(25) Filing Language:

English

(26) Publication Language:

English

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

(72) Inventors: ROENNOW, Troels; 61 Ellis Road, Cambridge CB2 9BG (GB). WABNIG, Joachim; 62 Halifax Road, Upper Cambourne CB23 6AX (GB). MARTÍN LÓPEZ, Enrique; 22b Carlyle Road, Cambridge CB4 3DN (GB).

(74) Agent: SEPPO LAINE OY; Itämerenkatu 3 A, 00180 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, DJ, 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, 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).

Declarations under Rule 4.17:

— of inventorship (Rule 4.17(iv))

Published:

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

(54) Title: ELECTRONIC DOCUMENTS MANAGEMENT

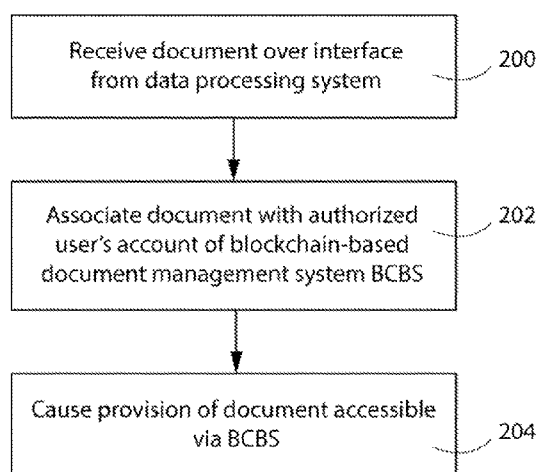


Fig. 2

(57) Abstract: According to an example aspect of the present invention, there is provided a method, comprising: receiving a document over an interface from a data processing system, associating the document with an authorized user's account of a blockchain-based document management system, and causing provision of the document accessible via the blockchain-based document management system.

ELECTRONIC DOCUMENTS MANAGEMENT

FIELD

[0001] The present invention relates to electronic documents management and in particular to integration of documents from legacy systems.

5

BACKGROUND

[0002] Digitalizing and integrating legacy records is a recurrent problem in electronic document records management (EDRM). Many businesses accumulate past records in formats that are not compatible with the methods that are commonly adopted nowadays. Such legacy records can range from storing paper hard copies, to digital records that became incompatible with a subsequent IT system, and were just put on hold and never migrated.

[0003] A further motivation for digitalizing legacy records is the increase in computational power and big data analytic capabilities. The Public Health sector in particular could greatly benefit from integrating legacy records with the more recent data that is already accessible in its present digital form. The availability of data sets ranging even hundreds of years could unveil statistical patterns that would help understanding correlations between different health conditions together with demographic information.

[0004] Apart from the benefits of applying modern Machine Learning algorithms to historical data, digitalizing legacy records will become important to meet the current demand of data ownership and accessibility. Consumers are more and more concerned about their personal data, which is scattered around different systems, not easily under their control, and even not always accessible to them. Besides, guaranteeing that the data comes from a trustable source (provenance) is an important aspect in current and future information technologies. There is need for improvements for enabling accessibility of legacy documents without compromising data privacy.

SUMMARY

[0001] The invention is defined by the features of the independent claims. Some specific embodiments are defined in the dependent claims.

[0002] According to a first aspect of the present invention, there is provided apparatus comprising at least one processing core, at least one memory including computer program code, the at least one memory and the computer program code being configured to, with the at least one processing core, cause the apparatus at least to: receive a document
5 over an interface from a data processing system, associate the document with an authorized user's account of a blockchain-based document management system, and cause provision of the document accessible via the blockchain-based document management system:

[0003] According to a second aspect of the present invention, there is provided a method, comprising: receiving a document over an interface from a data processing
10 system, associating the document with an authorized user's account of a blockchain-based document management system, and causing provision of the document accessible via the blockchain-based document management system.

[0004] According to an embodiment, the apparatus is caused to operate as a blockchain node and update state of the blockchain at least with the association.

15 [0005] According to an embodiment, the interface is a printer interface and the apparatus is configured to function as a printer towards a legacy data storage system.

[0006] According to an embodiment, the document is associated with a public encryption key of a public-secret encryption key pair that is comprised by the account in the blockchain-based document management system. A key value mapping associating
20 user's public encryption key with a key of the document may be generated, wherein the key of the document is a hash of at least a portion of the document.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] FIGURE 1 illustrates an example system capable of supporting at least some embodiments of the present invention;

25 [0008] FIGURE 2 illustrates a method in accordance with at least some embodiments of the present invention;

[0009] FIGURE 3 illustrates a method in accordance with at least some embodiments of the present invention;

[0010] FIGURE 4 illustrates a blockchain-based health record management system in accordance with at least some embodiments of the present invention;

[0011] FIGURE 5 illustrates a method in accordance with at least some embodiments of the present invention;

5 [0012] FIGURE 6 illustrates a method in accordance with at least some embodiments of the present invention, and

[0013] FIGURE 7 illustrates an apparatus in accordance with at least some embodiments of the present invention.

10

EMBODIMENTS

[0014] Innovative decentralized data storage solutions, such as blockchains enable provenance and avoid the need to rely on centralized third parties to regulate information and data systems. In addition, blockchain platforms can host “smart contracts” which could replace established methods based on human witnesses with logical software-implemented
15 protocols.

[0015] A blockchain is a distributed computing architecture where every network node executes and records the same transactions, which are grouped into blocks. Only one block can be added at a time, and every block contains a mathematical proof that verifies that it follows in sequence from the previous block. In this way, the blockchain’s
20 distributed database is kept in consensus across the whole network, and this is achieved without the need of a central authority. Nodes that maintain and verify the network are incentivized by mathematically enforced economic incentives coded into the protocol. The blockchains can work in different ways, as well as in different scales. Apart from keeping an immutable, comprehensive record of events, to be conveniently acted upon, blockchains
25 offer security in a complex network by accommodating consensus algorithms that are mathematically hard to corrupt.

[0016] There is now provided a method and apparatus enabling direct interface for integrating documents from legacy systems by applying blockchain technology. Documents from a legacy document management system or database are made accessible
30 in a blockchain-based document management system. The interfaced systems may be

public, private, or hybrid. For example, a database storing a huge amount of old data may run in a legacy operating system that is incompatible with modern blockchain software. A gateway device and a method are provided to interface blockchains directly with such legacy systems, and also with modern ones. Instead of manual transfer, documents in legacy systems can be easily made available in modern and highly secure blockchain based document management system. Provenance and auditability can be provided to any document brought to the BCBS. This provides substantial advantages in various fields, such as storage of patient records.

[0017] FIGURE 1 illustrates an example system in accordance with at least some embodiments of the present invention. A legacy data processing system 20 may comprise a computer with legacy operating system 21 and a legacy database 22 storing legacy documents. The term legacy data processing system is to be understood broadly and may cover various currently deployed and already phased-out data processing systems, such as patient record management systems, that are not part of the blockchain-based document management system. The legacy system 20 is connectable over an interface 23 to an interfacing apparatus, referred herein as a gateway device 10. The gateway device 10 connects the legacy system to a blockchain-based document management system or data storage system (BCBS) which may comprise a blockchain 30. The BCBS and the blockchain-based document management system may refer generally to a document storage solution utilizing a blockchain network 30.

[0018] Figure 1 illustrates that the gateway device 10 may belong to the blockchain 30 comprising blockchain nodes 31 and store local blockchain (BC) database 12. The gateway device may host a full blockchain node, making the device a part of the blockchain network that enables the BCBS. The BCBS may also comprise or be provided in a distributed file system (DFS) 40 which may also be decentralized and comprised of a series of nodes 41. In another embodiment, instead of the DFS 40 a centralized file system is used.

[0019] The nodes 12, 31 may comprise corporate, authority, and/or user devices, such as a server, a desktop/tablet/laptop computer, smartphone, set-top box or other suitable electronic device. The system may comprise an administrator or management node, a hub, relay or other kind of intermediate device for connecting a node to further networks or services, such as another distributed or centralized computing system or a

cloud service. The nodes are mutually addressable in a suitable way, for example, they may be connected to an internet protocol, IP, network. Messages released into the IP network with a recipient address are routed by the network to the recipient node identified by the recipient address. IP is not the only suitable networking technology used, for example, other peer-to-peer networking models are also suitable.

[0020] The blockchain state information shared by the nodes 12, 31 may store all the transactions and history carried out in the network, also regarding the documents imported from the legacy system 20. The blockchain state information is stored in or as a blockchain ledger. Each node comprises the ledger whose content is in sync with other ledgers. The nodes may validate and commit transactions in order to reach consensus. Each node may have their own copy of the ledger which is in some embodiments permission-controlled, so participants see only appropriate transactions. Changes in resource ownership take the form of transactions secured by strong cryptography. A transaction may comprise an identifier of a new owner, that is the recipient, of the resource, together with a cryptographic signature of the previous owner, that is the sender, such that malicious attackers cannot re-assign resources they do not own. Application of blockchain technology and the ledger enable a way to track the unique history of transactions by the individual nodes in the network. Blockchains could also enable smart devices to become independent agents, autonomously conducting a variety of transactions.

[0021] FIGURE 2 illustrates a method according to some embodiments. The method may be implemented in the gateway device 10, for example. A document is received 200 over an interface from a source data processing system, such as the legacy system 20. The document is associated 202 with an authorized user's account of the blockchain-based document management system. The authorized user refers to owner or controller of the data, such as a patient for his medical record. The user account generally refers to information associated with user, user-group or an authority, for example, typically including identification and encryption information. The document is provided 204 to be accessible via the BCBS. The gateway device 10 may, as a blockchain node update state of the blockchain at least with the association.

[0022] There are many available options how the document from the source system may be made accessible via blockchain-based storage, some of which are illustrated herewith. The document may be stored in connection with step 204 in encrypted form, in

the blockchain 30 and/or a further document storage system 40 accessible via the associated information stored in the blockchain. The gateway device 10 may be arranged to provide a file generated on the basis of the document to a DFS storage node 41 for storing at least a part of the file. In another embodiment, the gateway device 10 may function as a
5 DFS storage node and store 11 at least a file generated on the basis of the document. Such file may comprise the document or at least part of it. Additionally, a blockchain transaction regarding the imported document may be generated and the blockchain state updated.

[0023] With reference to FIGURE 3, some further embodiments are illustrated below. Some or all of the features illustrated in connection with Figure 3 may be
10 performed in an apparatus responsible for causing 204 addition of the document to the BCBS, such as the gateway device 10. The interface 23 may be a printer interface and the gateway device 10 may configured to function as a printer towards the legacy data storage system 20. The gateway device appearing as a printer may thus be accessible by standard printer drivers from the legacy operating systems by the computer 21 that has access to the
15 old documents in the legacy DB 22. The user of such device may access a document in the legacy database 22 and simply choose to print 302 the document to the printer 10. Since the gateway device 10 can cause the document to be accessible via the blockchain, the device may thus operate and be referred to as a blockchain printer or a blockchain document printer. This enables simple interface for users to transfer documents to the
20 BCBS with highly advanced properties i.e. regarding auditability. For example, a user may have an electronic file of a contract they want to store. By simply selecting printing to the blockchain printer the user can get the documents to the BCBS and can prove that the document existed at this moment in time.

[0024] The gateway device 10 may further perform an additional printing to paper
25 function, or be a standalone device without physical printer functionality. This enables, for instance, automatic addition of documents printed from a legacy system to a blockchain, which are associated with the authorized user e.g. by a public encryption key of the user. In another example embodiment, there is a further printer device enabling printing of documents from the legacy system for providing access to the blockchain based storage.
30 Such printer device may be connected to the gateway device 10 providing the document available in the BCBS. In another embodiment, the hardware contained in the printer device may include storage and the printer device may also be a node of the distributed BCBS system and provide the document accessible via the BCBS. The user may in 302

choose to actually print the document to paper or not. This may be simply a direct consequence of selecting the blockchain printer/gateway device 10 on the legacy computer 21 as the printer for the document.

[0025] In connection with step 302, or as a separate step, document format conversion may be carried out for at least part of the document, from a first format of the source system into a second format applied in the BCBS. This may be carried out by the gateway device 10, for example. The translation may involve change from Page Description Language (PDL), or any protocol used by the legacy system 20 to communicate with the gateway device 10, into the required format of the BCBS. PDL is a general class that includes for example PostScript (PS). In one example, the PDL may just be copied to the BCBS record. This would always work regardless of how old the legacy system is. If the records are recent enough so that text can be understood, such text can be incorporated into the BCBS record. This provides the advantage being able to search within the document. In a still further example an optical character recognition (OCR) system is applied to read from PDL into text for the BCBS record. However, these are just some examples of ways how the document may be modified prior to storing in the BCBS.

[0026] In some embodiments, public key encryption is applied for the document in the BCBS. When the authorized user chooses to add the document to the BCBS system, the user may provide a public key (pk) to associate the document to the user in the BCBS. The public key may be provided in connection with printing the 302 the document or it may be beforehand provided and associated with the user, for example. The public key can be provided in several ways: from being issued with the print command from the computer 21; to using an authorization command provided, for instance via Near Field Communication (NFC) by a wearable device enabling digital signatures or a smartphone that stores in an electronic wallet the public key or a public-secret key pair.

[0027] The document may be associated 202, 304 with the public encryption key pk of a public-secret encryption key pair that is comprised by the account of the authorized user in the blockchain-based document management system. In an embodiment, a key value L mapping the associating user's public encryption key pk with a key of the document ($file_key$) may be generated. The key of the document ($file_key$) may be a hash of at least a portion of the document. The key value L may be included in the state of the blockchain, synchronized across the blockchain nodes.

[0028] It is expected that the documents are typically stored in an encrypted form in the BCBS, and the document may be encrypted 306 with an encryption key of or associated with the authorized user for instance, by means of a patient's physical or virtual healthcare card. The gateway device 10 may encrypt the document as part of the process of
5 importing the document printed from the legacy system to the BCBS. There are various options for arranging encryption of the documents, such as asymmetric encryption, where the gateway device 10 may in step 306 perform public key encryption of the document by the public key of the authorized user. Another example option is encryption with a random key. In this embodiment, the gateway device 10 may compute the Diffie-Hellmann shared
10 secret between the authorized user's public key and the gateway device's key. A random number is then generated. The random number is used to encrypt 306 the document and the random number itself is encrypted using the Diffie-Hellmann shared secret which is then sent to the user over the network or via NFC. A still further option is to apply symmetric encryption. The authorized user's wallet may simply communicate its private key to the
15 gateway device 10 which uses the private key to encrypt 306 the document. This method requires that gateway device 10 is a trusted device and further security measures may be needed, such as tamper resistant casing, to maintain trust in devices.

[0029] In some embodiments, the contents of the document may be partitioned 308, divided or shred to a plurality of document parts. The document parts may thus be
20 provided to different nodes of the BCBS. This is an optional feature and may be carried out by the gateway device 10. At least one new transaction to the blockchain due to the import of the document is generated 310 and added 312 to the blockchain. In addition, the document (parts) is (are) distributed 312. In an embodiment, the blockchain state stored in the blockchain nodes 31 is updated with the key value *L*.

25 [0030] A DFS 40, which may be separate from the blockchain 30, may serve as an external storage and map the key of document (*file_key*) to the actual data file comprising the document (*file*), typically as encrypted. The BCBS system will likely work using a blockchain 30 with some amount of internal storage, keeping track of the subsequent states, and an external DFS storage 40. The blockchain and the DFS storage are comprised
30 of a series of nodes. In some embodiments, a system participating in the BCBS will host both a blockchain and a storage node, and this would be the case of the BCBS printer devices (as depicted for the gateway device 10 in Figure 1).

[0031] However, it is to be appreciated that the above is just one example of how the document may be associated 202 to the authorized user's account. Basically, the document may be associated with any feasible user-specific information, which the user can use to recover the document. For example, the authorized user may use a hash of his/her home
5 address, a random number or some other piece of information that the user thinks is memorable. A key management function or device may be used to take care of these associations, for example by public private key cryptography.

[0032] Once a new block including information on the imported document is established, the blockchain becomes longer. A transaction is considered the more reliable,
10 the larger the number of blocks established since the block where the transaction is comprised. This is since transactions are hashed into the chain of blocks, and discrepancies in the blockchain are resolved as the blockchain gets longer. In detail, maliciously modifying a transaction in a block far down the chain would involve re-doing the work of finding proofs for all subsequent blocks, since the input to the hash function for the block
15 comprising the transaction would be changed, causing the resulting hash value, with the proof in that block, to no longer be disposed in the desired area in the output space of the hash function.

[0033] An access rights management system is part of the BCBS system and allows to control who can write and read data, also regarding the documents imported from the
20 legacy system 20. Some further embodiments regarding access to the documents via blockchain are illustrated below. In response to receiving a blockchain-based access transaction request for the document, authorization of a party associated with the request may be checked on the basis of verifying a signature on the access request transaction. When public key cryptography is applied, the user's secret key is required in order to
25 decrypt the encrypted document via the blockchain 30 and/or the DFS 40.

[0034] In some embodiments, the document imported to the BCBS is a medical or health record or part hereof associated to patient's public encryption key or other identifier, and the blockchain 30 is used for access control to the medical records. FIGURES 4 to 6 illustrate some example embodiments for applying presently disclosed features for such
30 documents including sensitive medical information.

[0035] The gateway device 10 may import a legacy medical record and cause creation of a BCBS record 402. This may be done by applying at least some of the above

illustrated features. The record in this example embodiment is partitioned into parts 404a, 404b, and different parts of the medical record are stored in or for access via different BCBS nodes 31a, 31b, 41. When a practitioner, such as a doctor, needs access to a patient record, in response to such input to a user interface of a computer 410 directly or indirectly
5 connected to the blockchain 30 and/or the DFS 40, a corresponding data access transaction request is sent to and received 502 by a blockchain node. Any node belonging to the BCBS and storing at least part of the document may detect the request and carry out the features illustrated in connection with Figure 5.

[0036] Authorization of a healthcare practitioner is checked 504 in response to an
10 access request transaction to at least part of the patient's medical record. For example, the node may verify that the request was made by a certified doctor. This may be done by verifying that the signature on the transaction matches a public key of a certified doctor maintained in the blockchain database 30.

[0037] In an embodiment, the node is also required to verify 506 (an optional step)
15 that the patient has given his or her consent, for example by checking that the public encryption key associated to the record matches the patient signature received with the request 502. If step 508 concludes that the criteria 504 and/or 506 for accessing the document (part) is fulfilled, the requested patient record or record part is sent 510 to the requesting node. The record parts can be accessed via the blockchain and further shown
20 412 for the practitioner. If the access criteria is not fulfilled, the request is rejected 512. Hence, secret patient data can be stored as encrypted and distributed, and blockchains are used for access control.

[0038] FIGURE 6 further illustrates an embodiment for accessing a document, such a patient record 402, stored in the BCBS. The method may be applied in a device
25 connected to a blockchain, such as the device 410, or a device functioning as a node of the blockchain, such as the gateway device 10. There may be specific access control verification upon receiving 602 a request for such document, such as a check of the practitioner's credentials, typically his public encryption key, at the computer 410 being used. However, this may be optional, since there may be access permission control
30 performed by the blockchain node(s) storing the document (or part thereof) and/or later before providing the record to the requesting party. The request may be signed 604 by practitioner's digital signature. The request may optionally also be signed by patient's

digital signature in case patient's explicit consent is a pre-requisite for accessing the record in the BCBS. The signature may be generated with a smartcard, a wearable, a token, a private key on a computer, mobile terminal or any other device capable of making a digital signature.

5 [0039] The signed request for the document is sent 606 to the blockchain. The document data is received 608 from at least one blockchain node. Block 610 illustrates that the request (and/or subsequent access to the document) may be optionally stored on the blockchain upon receiving the request. Thus, the state of the blockchain is updated with information on the access request to the medical record, enabling to track each access
10 request to the patient record.

 [0040] In some embodiments, the document in encrypted form is decrypted 612 on the basis of a secret encryption key in a memory module of the patient, such as a token, a healthcare card, a wearable, a subscriber identification module, or a mobile
15 healthcare card and can only be decrypted 612 with it. The healthcare card may interact with the doctor's computer using a normal smart card reader, NFC or other suitable communication method. The requested patient document (or part thereof) to be shown may be compiled and provided 614 for the requesting party.

 [0041] Figure 4 illustrates an example where the document may be shown 412 to the
20 practitioner on his computer 410 connected to the gateway device 10, which may function as the blockchain printer. The gateway device 10 may thus carry out the features illustrated in Figure 6 and also provide access to the documents imported to the BCBS from the legacy system 20. However, it is to be understood that this is just one example of how the access may be arranged. For example, the practitioner's computer 410 may also be
25 arranged to function as a blockchain node and be directly connected to the BCBS and/or comprise the gateway device 10.

 [0042] FIGURE 7 illustrates an example apparatus capable of supporting at least some embodiments of the present invention. Illustrated is a device 700, which may comprise a communications device arranged to operate as a node in a blockchain-based
30 storage. The device may be arranged to carry out at least some of the embodiments related to interfacing with a legacy data processing system and/or providing documents accessible via a blockchain-based storage illustrated above. The device may include one or more

controllers configured to carry out operations in accordance with at least some of the embodiments illustrated above, such as some or more of the method steps illustrated in connection with Figures 1 to 6. For example, the device may operate as the gateway device 10.

5 [0043] Comprised in the device 700 is a processor 702, which may comprise, for example, a single- or multi-core processor wherein a single-core processor comprises one processing core and a multi-core processor comprises more than one processing core. The processor 702 may comprise more than one processor. The processor may comprise at least one application-specific integrated circuit, ASIC. The processor may comprise at least one
10 field-programmable gate array, FPGA. The processor may be means for performing method steps in the device. The processor may be configured, at least in part by computer instructions, to perform actions.

[0044] The device 700 may comprise memory 704. The memory may comprise random-access memory and/or permanent memory. The memory may comprise at least
15 one RAM chip. The memory may comprise solid-state, magnetic, optical and/or holographic memory, for example. The memory may be at least in part accessible to the processor 702. The memory may be at least in part comprised in the processor 702. The memory 704 may be means for storing information. The memory may comprise computer instructions that the processor is configured to execute. When computer instructions
20 configured to cause the processor to perform certain actions are stored in the memory, and the device in overall is configured to run under the direction of the processor using computer instructions from the memory, the processor and/or its at least one processing core may be considered to be configured to perform said certain actions. The memory may be at least in part comprised in the processor. The memory may be at least in part external
25 to the device 700 but accessible to the device. Network state information, as well as control parameters affecting operations in the BCBS may be stored in one or more portions of the memory and used to control operation of the apparatus in the BCBS and/or to import documents from the legacy data processing system.

[0045] The device 700 may comprise a transmitter 706. The device may comprise a
30 receiver 708. The transmitter and the receiver may be configured to transmit and receive, respectively, information in accordance with at least one wired or wireless, cellular or non-cellular standard. The transmitter may comprise more than one transmitter. The receiver

may comprise more than one receiver. The transmitter and/or receiver may be configured to operate in accordance with global system for mobile communication, GSM, wideband code division multiple access, WCDMA, long term evolution, LTE, IS-95, wireless local area network, WLAN, Ethernet and/or worldwide interoperability for microwave access, 5 WiMAX, standards, for example. The device 700 may comprise a near-field communication, NFC, transceiver 710. The NFC transceiver may support at least one NFC technology, such as NFC, Bluetooth, Wibree or similar technologies.

[0046] The device 700 may comprise user interface, UI, 712. The UI may comprise at least one of a display, a keyboard, a touchscreen, a vibrator arranged to signal to a user 10 by causing the device to vibrate, a speaker and a microphone. A user may be able to operate the device via the UI, for example to accept incoming telephone calls, to originate telephone calls or video calls, to browse the Internet, to manage digital files stored in the memory 704 or on a cloud accessible via the transmitter 706 and the receiver 708, or via the NFC transceiver 710, and/or to play games.

15 [0047] The device 700 may comprise or be arranged to accept a user identity module or other type of memory module 714. The user identity module may comprise, for example, a subscriber identity module, SIM, and/or a healthcare IC card installable in the device 700. The user identity module 714 may comprise information identifying a subscription of a user of device 700. The user identity module 714 may comprise 20 cryptographic information usable to verify the identity of a user of device 700 and/or to facilitate encryption and decryption of documents and communication effected via the device 700, such as the private and/or public keys as illustrated above.

[0048] The processor 702 may be furnished with a transmitter arranged to output information from the processor, via electrical leads internal to the device 700, to other 25 devices comprised in the device. Such a transmitter may comprise a serial bus transmitter arranged to, for example, output information via at least one electrical lead to memory 704 for storage therein. Alternatively to a serial bus, the transmitter may comprise a parallel bus transmitter. Likewise the processor may comprise a receiver arranged to receive information in the processor, via electrical leads internal to the device 700, from other 30 devices comprised in the device 700. Such a receiver may comprise a serial bus receiver arranged to, for example, receive information via at least one electrical lead from the

receiver 708 for processing in the processor. Alternatively to a serial bus, the receiver may comprise a parallel bus receiver.

[0049] The device 700 may comprise further devices not illustrated in Figure 7. For example, the device may comprise at least one digital camera. Some devices may comprise
5 a back-facing camera and a front-facing camera. The device may comprise a fingerprint sensor arranged to authenticate, at least in part, a user of the device. In some embodiments, the device lacks at least one device described above. For example, some devices may lack the NFC transceiver 710 and/or the user identity module 714.

[0050] The processor 702, the memory 704, the transmitter 706, the receiver 708, the
10 NFC transceiver 710, the UI 712 and/or the user identity module 714 may be interconnected by electrical leads internal to the device 700 in a multitude of different ways. For example, each of the aforementioned devices may be separately connected to a master bus internal to the device, to allow for the devices to exchange information. However, as the skilled person will appreciate, this is only one example and depending on
15 the embodiment various ways of interconnecting at least two of the aforementioned devices may be selected without departing from the scope of the present invention.

[0051] It is to be understood that the embodiments of the invention disclosed are not limited to the particular structures, process steps, or materials disclosed herein, but are extended to equivalents thereof as would be recognized by those ordinarily skilled in the
20 relevant arts. It should also be understood that terminology employed herein is used for the purpose of describing particular embodiments only and is not intended to be limiting.

[0052] References throughout this specification to one embodiment or an embodiment means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of the present
25 invention. Thus, appearances of the phrases “in one embodiment” or “in an embodiment” in various places throughout this specification are not necessarily all referring to the same embodiment. The skilled person will appreciate that above-illustrated embodiments may be combined in various ways. Embodiments illustrated in connection with Figures 3 to 6 may be taken in isolation or further combined together. For example, with reference to Figure 3, use of public key encryption may be applied separately from the embodiment of printing
30 the document in Figure 3. As another example, some or all of the features illustrated in

connection with Figures 4 to 6 may be applied for other types of documents than patient records.

[0053] Various embodiments and examples of the present invention may be referred to herein along with alternatives for the various components thereof. It is understood that
5 such embodiments, examples, and alternatives are not to be construed as de facto equivalents of one another, but are to be considered as separate and autonomous representations of the present invention.

[0054] Furthermore, the described features, structures, or characteristics may be combined in any suitable manner in one or more embodiments. In the preceding
10 description, numerous specific details are provided, such as examples of lengths, widths, shapes, etc., to provide a thorough understanding of embodiments of the invention. One skilled in the relevant art will recognize, however, that the invention can be practiced without one or more of the specific details, or with other methods, components, materials, etc. In other instances, well-known structures, materials, or operations are not shown or
15 described in detail to avoid obscuring aspects of the invention.

[0055] While the forgoing examples are illustrative of the principles of the present invention in one or more particular applications, it will be apparent to those of ordinary skill in the art that numerous modifications in form, usage and details of implementation can be made without the exercise of inventive faculty, and without departing from the
20 principles and concepts of the invention. Accordingly, it is not intended that the invention be limited, except as by the claims set forth below.

[0056] The verbs “to comprise” and “to include” are used in this document as open limitations that neither exclude nor require the existence of also un-recited features. The features recited in depending claims are mutually freely combinable unless otherwise
25 explicitly stated. Furthermore, it is to be understood that the use of “a” or “an”, that is, a singular form, throughout this document does not exclude a plurality.

INDUSTRIAL APPLICABILITY

At least some embodiments of the present invention find industrial application in
30 communications.

ACRONYMS LIST

	ASIC	Application-specific integrated circuit
	BCBS	Blockchain-based storage
	DC	Direct current
5	EDRM	Electronic document records management
	FPGA	Field-programmable gate array
	GSM	Global system for mobile communication
	IC	Integrated Circuit
	LTE	Long term evolution
10	M2M	Machine-to-machine
	NFC	Near-field communication
	OCR	Optical character recognition
	P2P	Peer-to-peer
	PDL	Page Description Language
15	PoS	Proof-of-stake
	PoW	Proof-of-work
	PS	PostScript
	UI	User interface
	WCDMA	Wideband code division multiple access,
20	WiMAX	Worldwide interoperability for microwave access
	WLAN	Wireless local area network

CLAIMS:

1. An apparatus comprising at least one processing core, at least one memory including computer program code, the at least one memory and the computer program code being
5 configured to, with the at least one processing core, cause the apparatus at least to:
 - receive a document over an interface from a data processing system,
 - associate the document with an authorized user's account of a blockchain-based document management system, and
 - cause provision of the document accessible via the blockchain-based document
10 management system.
2. The apparatus of claim 1 wherein the apparatus is caused to operate as a blockchain node and update state of the blockchain at least with the association.
- 15 3. The apparatus of claim 1 or 2, wherein the interface is a printer interface and the apparatus is configured to function as a printer towards a legacy data storage system.
4. The apparatus of any preceding claim, wherein the apparatus is further configured to receive the document in a first format, and convert at least part of the document into a
20 second format of the blockchain-based document management system.
5. The apparatus of any preceding claim, wherein the document is associated with a public encryption key of a public-secret encryption key pair that is comprised by the account in the blockchain-based document management system.
25
6. The apparatus of claim 5, wherein the apparatus is configured to generate a key value mapping associating user's public encryption key with a key of the document, wherein the key of the document is a hash of at least a portion of the document.
- 30 7. The apparatus of claim 6, wherein the key value is included in the state of the blockchain, synchronized across the blockchain nodes.

8. The apparatus of any preceding claim, wherein the apparatus is configured to function as a distributed file system storage node storing at least a file generated on the basis of the document, or
the apparatus is configured to provide a file generated on the basis of the document to a distributed file system storage node for storing at least a part of the file.

9. The apparatus of any preceding claim, wherein the apparatus is configured to partition the contents of the document to a plurality of document parts, and the document parts are provided to different nodes of the blockchain-based document management system.

10

10. The apparatus of any preceding claim, wherein the apparatus is configured to carry at least one of: encrypt the document by an encryption key of the user provided to the apparatus before provision to the blockchain-based document management system and decrypt the document received from the blockchain-based document management system by a decryption key of the user provided to the apparatus.

15

11. The apparatus of any preceding claim, wherein the apparatus is configured to, in response to receiving a blockchain-based access transaction request for the document, check authorization of a party associated with the request on the basis of verifying a signature on the access request transaction.

20

12. The apparatus of any preceding claim, wherein the document is a medical record associated to a patient and the apparatus is configured to use the blockchain for access control to the medical records.

25

13. The apparatus of claim 10, 11, and 12, wherein the apparatus is configured to perform at least one of:
check authorization of a healthcare practitioner and consent of the patient in response to an access transaction request to at least part of the patient's medical record,
decrypt the document in encrypted form on the basis of a secret encryption key in a memory module of the patient, and
update the state of the blockchain with information on the access request to the medical record.

30

14. A method, comprising:

- receiving a document over an interface from a data processing system,
- associating the document with an authorized user's account of a blockchain-based document management system, and
- 5 – causing provision of the document accessible via the blockchain-based document management system.

15. The method of claim 14, wherein the receiving, the associating, and the causing are carried out by an apparatus is caused to operate as a blockchain node and update state of
10 the blockchain at least with the association.

16. The method of claim 14 or 15, wherein the interface is a printer interface and the document is received by a printing operation from a legacy data storage system.

15 17. The method of any preceding claim 14 to 16, wherein the document is received in a first format, and at least part of the document is converted into a second format of the blockchain-based document management system.

18. The method of any preceding claim 14 to 17, wherein the document is associated with
20 a public encryption key of a public-secret encryption key pair that is comprised by the account in the blockchain-based document management system.

19. The method of any preceding claim 14 to 18, further comprising generating a key value mapping associating user's public encryption key with a key of the document, wherein the
25 key of the document is a hash of at least a portion of the document.

20. The method of claim 19, wherein the key value is included in the state of the blockchain, synchronized across the blockchain nodes.

30 21. The method of any preceding claim 14 to 20, wherein the document is provided for access to a distributed file system storage node storing at least a file generated on the basis of the document.

22. The method of any preceding claim 14 to 21, wherein the contents of the document is partitioned to a plurality of document parts, and the document parts are provided to different nodes of the blockchain-based document management system.
- 5 23. The method of any preceding claim 14 to 22, further comprising at least one of: encrypting the document by an encryption key of the user before provision to the blockchain-based document management system and decrypting the document received from the blockchain-based document management system by a decryption key of the user.
- 10 24. The method of any preceding claim 14 to 23, further comprising, in response to receiving a blockchain-based access transaction request for the document, checking authorization of a party associated with the request on the basis of verifying a signature on the access request transaction.
- 15 25. The method of any preceding claim 14 to 24, wherein the document is a medical record associated to a patient and the blockchain is used for access control to the medical records.
26. The method of claim 23, 24, and 25, further comprising at least one of:
checking authorization of a healthcare practitioner and consent of the patient in response to
20 an access transaction request to at least part of the patient's medical record,
decrypting the document in encrypted form on the basis of a secret encryption key in a memory module of the patient, and
updating the state of the blockchain with information on the access request to the medical record
- 25 27. An apparatus, comprising means for carrying out the method of any one of claims 14 to 26.
28. A non-transitory computer readable medium having stored thereon a set of computer
30 readable instructions that, when executed by at least one processor, cause an apparatus to perform the method of any one of claims 14 to 26.
29. A computer program configured to cause a method in accordance with at least one of claims 14 to 26 to be performed.

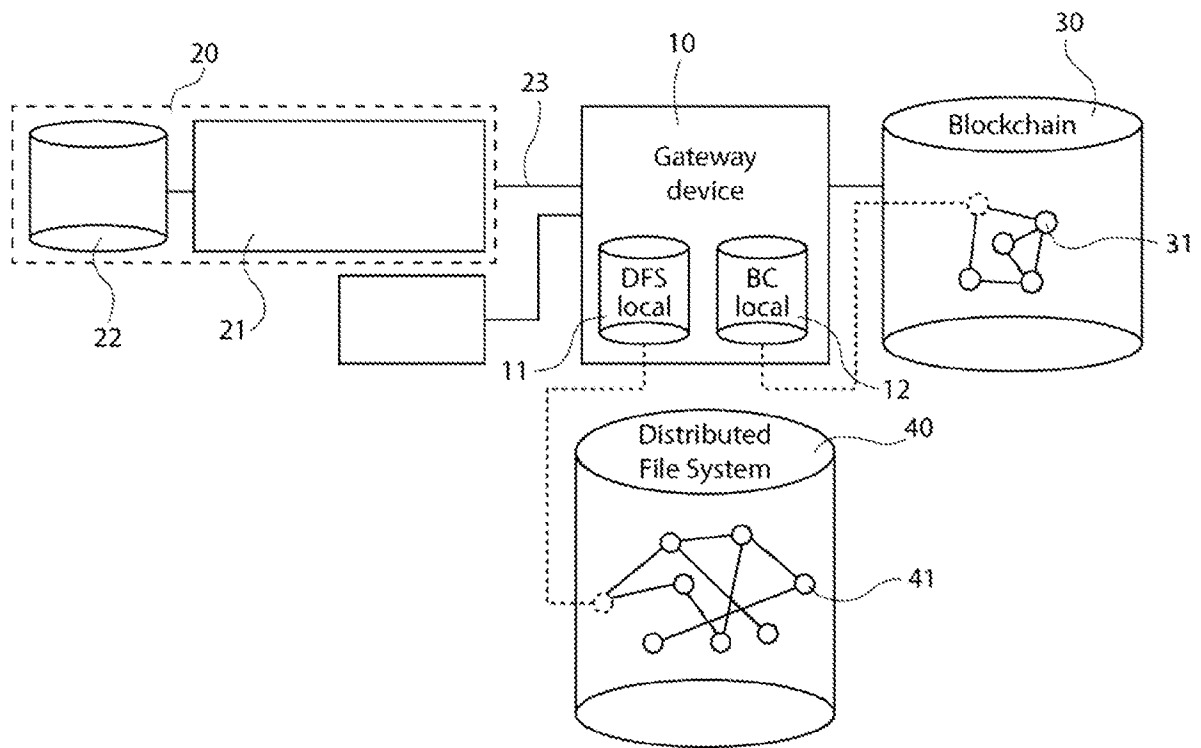


Fig. 1

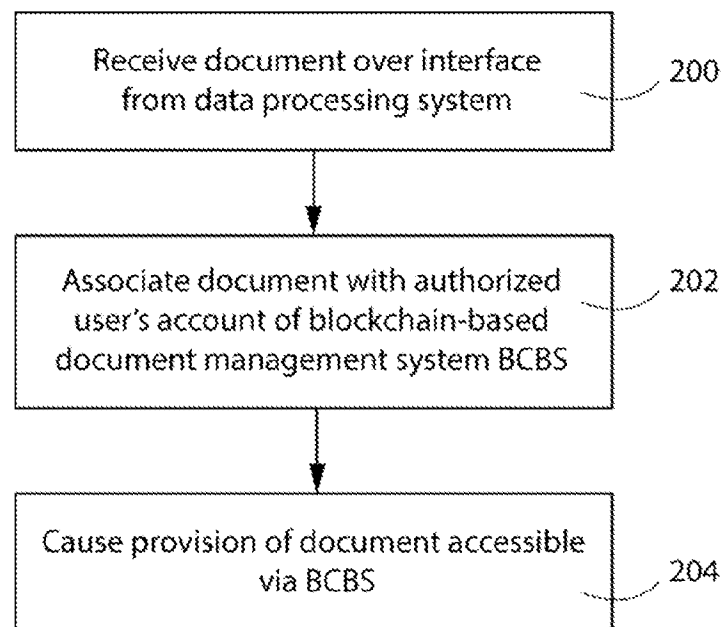


Fig. 2

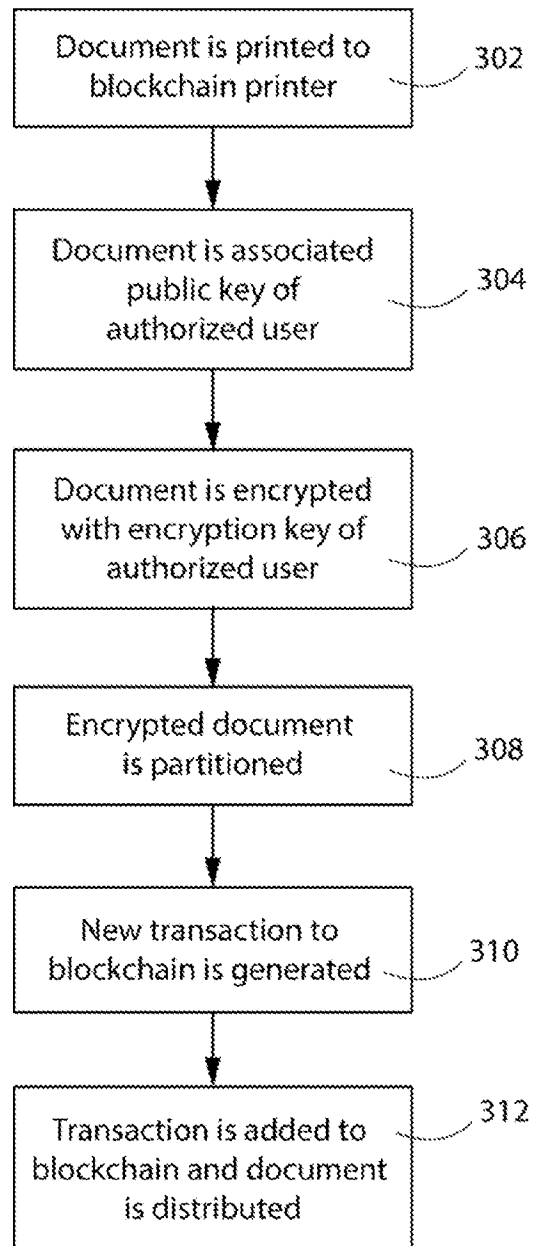


Fig. 3

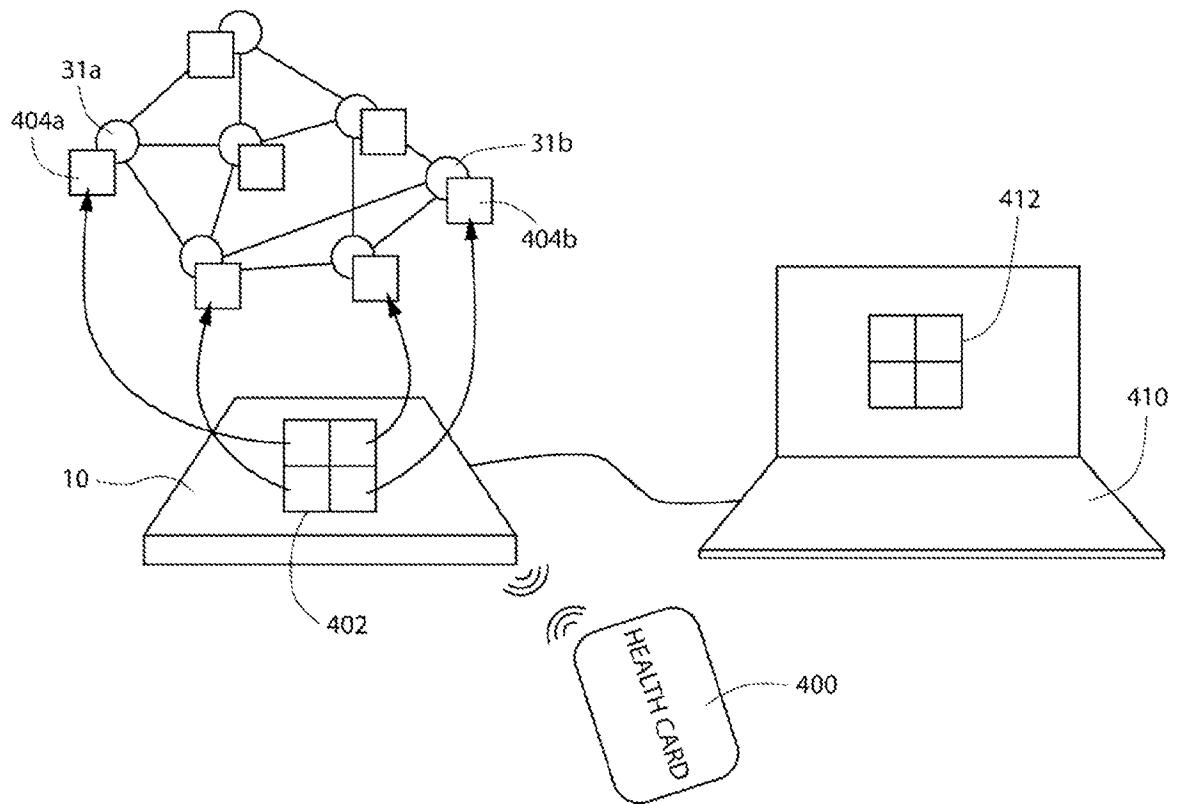


Fig. 4

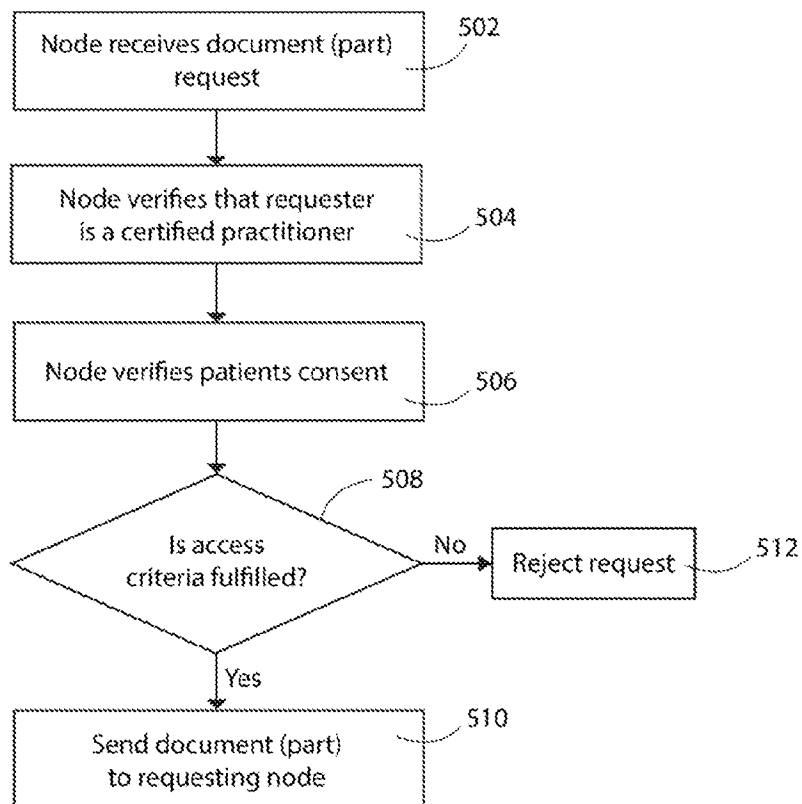


Fig. 5

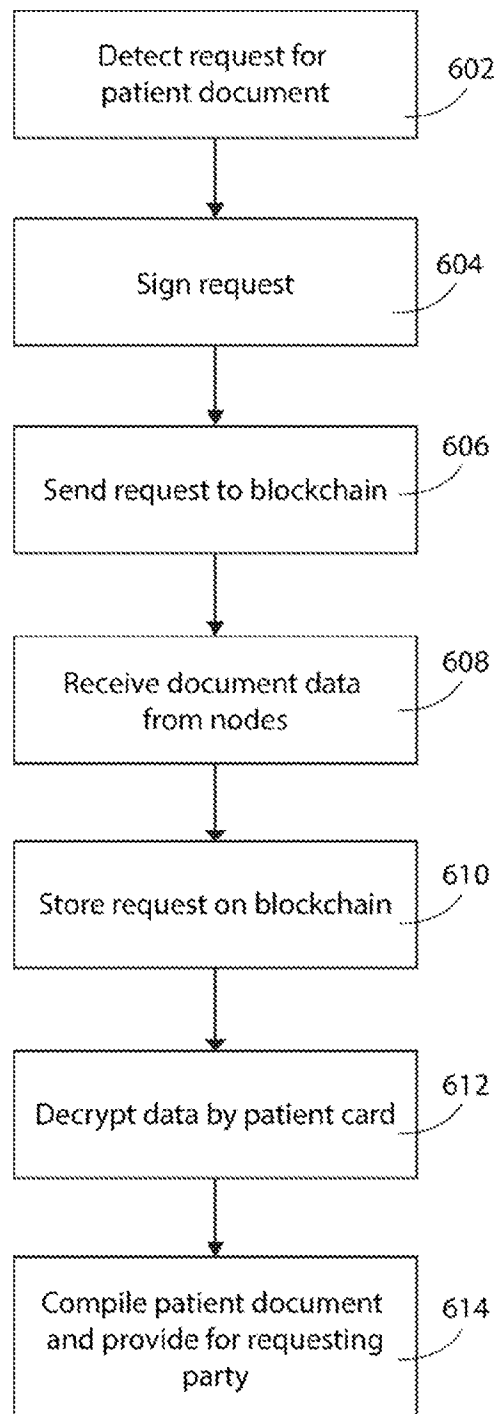


Fig. 6

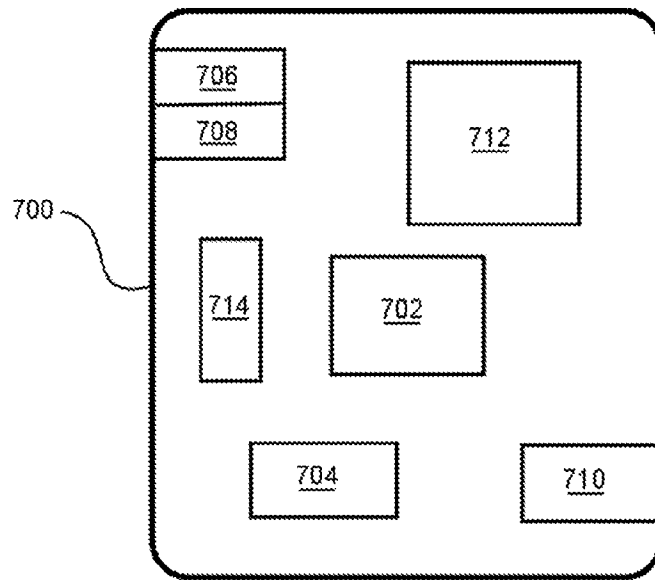


Fig. 7

INTERNATIONAL SEARCH REPORT

International application No.

PCT/FI2016/050841

A. CLASSIFICATION OF SUBJECT MATTER

See extra sheet

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)

IPC: G06F, G06Q

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

FI, SE, NO, DK

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

EPO-Internal, WPIAP, XPAIP, XPESP, XPI3E, XPIEE, XPIOP, XPIPCOM, XPMISC, XPOAC, XPRD, XPTK, COMPD, INSPEC, PUBCOMP, PUBSUBS, TDB, NPL

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	AZARIA, A. et al., "MedRec: Using Blockchain for Medical Data Access and Permission Management". In: Proceedings of the 2nd International Conference on Open and Big Data (OBD), 22-24 August 2016, pp. 25-30. XP032969608 Abstract; Figs. 1, 2; sections I, III A., B. and C. on pages 25-29	1-29
X	US 2016306982 A1 (SEGER II ROBERT A [US] et al.) 20 October 2016 (20.10.2016) Abstract; Figs. 1-3; claim 1; paragraphs [0015], [0016], [0063]-[0076]	1-29



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier application or patent but published on or after the international filing date	"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
"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)	"&" document member of the same patent family
"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	

Date of the actual completion of the international search

02 March 2017 (02.03.2017)

Date of mailing of the international search report

07 March 2017 (07.03.2017)

Name and mailing address of the ISA/FI
Finnish Patent and Registration Office
P.O. Box 1160, FI-00101 HELSINKI, Finland
Facsimile No. +358 9 6939 5328

Authorized officer
Vesa-Matti Louekoski
Telephone No. +358 9 6939 500

INTERNATIONAL SEARCH REPORT

International application No.

PCT/FI2016/050841

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	BURNISKE, C. et al., "How Blockchain Technology Can Enhance EHR Operability". ARK Invest & Gem, 29 September 2016. [Retrieved on 2017-03-01]. Retrieved from the Internet: <URL:http://research.ark-invest.com/blockchain-and-healthcare> The whole document	
A	WO 2016168922 A1 (BESSETTE LUC [CA]) 27 October 2016 (27.10.2016) page 30, line 28 – page 31, line 9	

INTERNATIONAL SEARCH REPORT
Information on Patent Family Members

International application No.
PCT/FI2016/050841

Patent document cited in search report	Publication date	Patent family members(s)	Publication date
US 2016306982 A1	20/10/2016	US 9397985 B1 WO 2016200456 A1	19/07/2016 15/12/2016
.....			
WO 2016168922 A1	27/10/2016	None	
.....			

INTERNATIONAL SEARCH REPORT

International application No.

PCT/FI2016/050841

CLASSIFICATION OF SUBJECT MATTER

IPC

G06F 17/30 (2006.01)

G06F 3/06 (2006.01)

G06Q 20/22 (2012.01)

G06Q 20/38 (2012.01)

G06Q 20/06 (2012.01)

G06Q 50/24 (2012.01)