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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 October 2017 (19.10.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/177260 A1

(51) International Patent Classification:
G06Q 20/40 (2012.01)

(21) International Application Number:
PCT/AU2017/000090

(22) International Filing Date:
13 April 2017 (13.04.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2016901453 13 April 2016 (13.04.2016) AU

(71) Applicant: **HAVENTEC PTY LTD** [AU/AU]; Level 27, 1 Market Street, Sydney NSW 2000 (AU).

(72) Inventor: **RICHARDSON, Ric B**; 1 Alcorn St, Suffolk Park NSW 2481 (AU).

(74) Agent: **WALLINGTON-DUMMER PATENT AND TRADE MARK ATTORNEYS**; PO Box 3888, Sydney NSW 2001 (AU).

(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, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Published:

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

(54) Title: SYSTEM OF SECURITY USING BLOCKCHAIN PROTOCOL

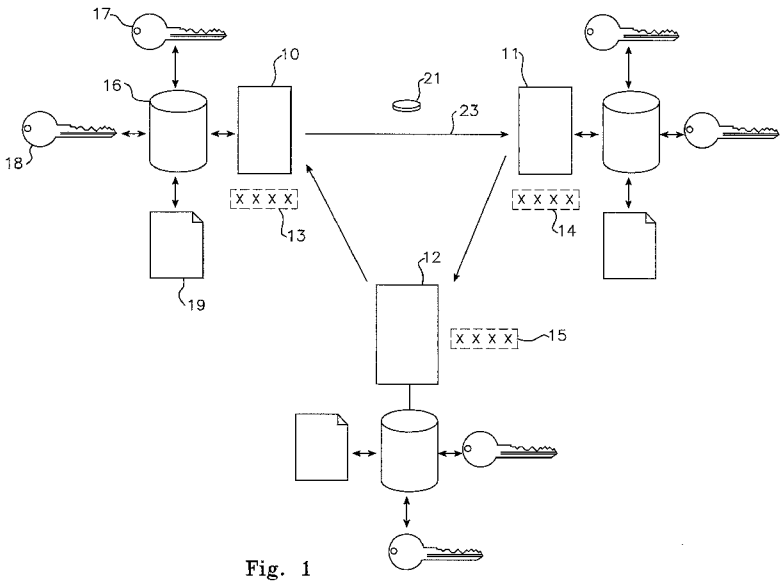

Fig. 1

(57) Abstract: A data record structure adapted for transmission over a network; the data record generated on a network device participating in a Blockchain which has an device unique identifier; the data record structure containing at least a first record and a first unique identifier record; the first record containing data for transmission over the network to a device having a receiving device unique identifier; the first unique identifier record containing the device unique identifier. Also disclosed is a method of verification of identity of devices participating in a block chain; said Block chain comprising a plurality of ledgers held on a plurality of network devices; said network devices communicating contents of the ledgers between them over a network; said devices verifying the contents of the ledgers as part of the step of communicating the contents of the ledgers; said method comprising incorporating a unique identifier of a network device within the ledger maintained by the network device.

WO 2017/177260 A1

System of security using BlockChain protocol

TECHNICAL FIELD

[0001] The present invention relates to a methodology and system components for attributing trust in network devices operating in a block chain environment. In an aspect it relates to the field of data record structures and, more particularly although not exclusively to those structures when used as part of a system for transmission of information using a block chain protocol which encapsulates specified data relating to the unique identity of at least a sending entity or device.

BACKGROUND

[0002] BitCoin and the BlockChain protocol are well known in the art. Principally the protocol has been used for applications in a state independent currency. Due to its highly secure nature and inherent mathematical integrity, the protocol is also an ideal opportunity for security applications although to date it has not been used as such.

[0003] In traditional use the BlockChain is a documented history of transactions showing both seller and buyer of tokens of value over time with an inbuilt ability to minimise the opportunity for fraudulent activity such as double spending of tokens.

[0004] Block chain structures in the context of initial use for Bitcoin storage and transactions is discussed in the publication: MultiChain Private Blockchain — White Paper by Dr Gideon Greenspan, Founder and CEO, Coin Sciences Ltd-available in the Wayback archive <http://web.archive.org/web/20160403063334/http://www.multichain.com/download/MultiChain-White-Paper.pdf >retrieved from Internet published on 3 April 2016 as per wayback engine. The full disclosure of this document is incorporated herein by cross-reference including the following portions which are specifically quoted:

"Bitcoin is now recognized as a cheap, rapid and reliable method for moving economic value across the Internet in a peer to peer manner.

BLOCKCHAINS AND TOKENIZATION

[0005] At the heart of bitcoin lies the blockchain, a global decentralized ledger which stores the full history of all bitcoin transactions. The blockchain is verified and stored by every node in the bitcoin network, of which there are approximately 6,000 in June 2015. The bitcoin protocol ensures that, barring temporary discrepancies, every node in the network has the same version of the blockchain, without requiring this consensus to be determined by a central authority. Another key feature of bitcoin (and the Blockchain structure) is that nodes can join or leave the network at any time, without disrupting the functioning of other nodes or the ongoing processing of transactions. New transactions can be created by any node and are propagated across the network in a Peer to peer fashion. Any node can take a set of these pending transactions and create ("mine") a new block containing them together with a link to the previous block. The new block "confirms" the transactions and is also propagated across the network. To prevent minority control over mining, bitcoin uses "proof of work" to make it computationally difficult and expensive to create a new block.

[0006] If a "fork" occurs, in which two competing blocks are mined almost simultaneously, proof of work also acts as a dispute resolution mechanism. Since blocks are hard to create, it is unlikely that both forks will grow at an identical speed. The protocol specifies that the fork with the greater amount of work is the correct one, so the network quickly regains a unified global consensus.

[0007] Along with bitcoin transactions, the blockchain can be used to store any digital data. While some view such uses as "bloating the blockchain", bitcoin's decentralized nature means that they cannot effectively be stopped. This led the developers of Bitcoin Core, the official bitcoin client, to introduce an official mechanism for adding arbitrary metadata to transactions in early 20143. This mechanism is used by services such as Proof of Existence and BlockSign to notarize the existence of a document by embedding a digital signature of that document inside a transaction. Other tools such as phpOP_RETURN enable larger pieces of data to be stored and retrieved from the blockchain, turning it into a general purpose permanent decentralized data store."

[0008] A feature of the design of the BitCoin network is the innate security of a wallet that is secured by public key encryption where the private key of the public key pair is kept secret. The wallet and therefore the owner of the wallet is identified by its public key. This is known in the art. The concern is that whilst the block chain structure provides security of data contained within the wallet there may exist a vulnerability to compromise in the network device or device which houses

the wallet and otherwise forms part of or participates in the block chain.

[0009] For example the entire network device may be replaced without other participating members of the block chain being aware that this has happened. This can lead to spoofing or equivalent vulnerabilities.

[00010] It is an object of the present invention to seek to improve the integrity of network devices or devices forming nodes in a block chain and thereby to improve the integrity of the block chain and the data stored and transmitted within it.

[00011] It is observed that there are other identifiers of a user or more specifically their device participating in the Blockchain. Identifiers available for verification of identity may include for example a device's IP number on a public or private network. Heretofor these have not been utilised to assist in improving the integrity of network devices or devices within the block chain.

[00012] Including this information in a transaction record such as the BlockChain may allow additional applications to be made of the BlockChain protocol.

NOTES

[00013] The term "comprising" (and grammatical variations thereof) is used in this specification in the inclusive sense of "having" or "including", and not in the exclusive sense of "consisting only of".

[00014] The above discussion of the prior art in the Background of the invention, is not an admission that any information discussed therein is citable prior art or part of the common general knowledge of persons skilled in the art in any country.

BRIEF DESCRIPTION OF INVENTION

[00015] Accordingly, in one broad form of the invention, there is provided a data record structure adapted for transmission over a network; the data record structure generated at an initiating device which has an initiating device IP address; the data record structure containing at least a first record and a first IP address record; the first record containing data for transmission over the network to a device having a receiving device IP address; the first IP address record containing the initiating device IP address.

[00016] In a further broad form of the invention there is provided a data record structure adapted for transmission over a network; the data record generated on a network device participating in a Blockchain which has a device unique identifier; the data record structure containing at least a first record and a first unique identifier record; the first record containing data for transmission over the network to a device having a receiving device unique identifier; the first unique identifier record containing the device unique identifier.

[00017] Preferably data from or pertaining to the first record is contained in a ledger.

[00018] Preferably the data record structure is contained within a wallet.

[00019] Preferably the data record structure further includes a second IP address record.

[00020] Preferably the second IP address record contains the receiving device IP address.

[00021] Preferably the data record structure further includes a second record.

[00022] Preferably the data record structure further includes a third record.

[00023] Preferably the first record contains token identifying data which uniquely identifies a token.

[00024] Preferably the token is exchanged between the initiating device and the receiving device.

[00025] Preferably the second record contains data which uniquely identifies a sending party.

[00026] Preferably the third record contains data which uniquely identifies a receiving party.

[00027] Preferably the data record structure further includes a hash range.

[00028] In yet a further broad form of the invention there is provided a transmission system for transmission of the data record structure defined above.

[00029] Preferably the data record structure is stored on an intermediate database as an intermediate database record.

[00030] Preferably a hash of the data record structure is stored on the intermediate database as part of the intermediate database record.

[00031] Preferably the intermediate database record is stored on a plurality of intermediate databases; each intermediate database separate and distinct from any other of the plurality of intermediate databases.

[00032] Preferably the plurality of intermediate databases form part of a BlockChain network.

[00033] Preferably the data record structure is accompanied by a public key which is shared with the rest of the network for identification, encryption and decryption purposes.

[00034] Preferably the data record structure includes a private key which is used for authentication, encryption and decryption purposes.

[00035] Preferably the wallet also has access to a transaction ledger which uses block chain protocols to remain in sync with other ledgers in the network.

[00036] Preferably when a token is received by a wallet, the token is then re routed to another wallet which also has its own public key, private key and associated ledger.

[00037] Preferably when a token is sent from one wallet to another, information about the transaction is recorded in ledgers including but not limited to the identity of the token, the identity of both the sending and receiving wallets, and the time of the transaction.

[00038] Preferably the IP numbers of both the sending and receiving device are also recorded in the transaction ledger thereby to establish and maintain a history of ownership and integrity of association between the IP number and a secure wallet.

[00039] Preferably the history of trust can be used to detect attempts to impersonate a device on the network.

[00040] Preferably the above described system incorporates an automatic resend capability.

[00041] Preferably when a wallet receives a token from another wallet, a timer and timing mechanism is set to automatically forward the token on to another device on the network.

[00042] Preferably the timing mechanism ensures that all devices on the network receive a regular delivery of tokens and helps to ensure that the transaction ledger remains current and active.

[00043] Preferably the wallet also has built in rules that are used to define if the wallet will receive or reject tokens that are sent to it.

[00044] Preferably if the IP number of the device sending the token does not exist in the transaction ledger then the system rejects the transaction.

[00045] Preferably if the token identity is not known and not in the ledger then the system rejects the token.

[00046] Preferably if the IP address recorded in the transaction record of the sending device does not match the IP address of the device sending the token, then the token is rejected by the system.

[00047] Preferably when the timing mechanism sends a token on to another device in the network, the system is programmed to send the token to the network device that has not had a delivery of a token for the longest time thereby to ensure that all devices on the network get a good average of transactions over time.

[00048] Preferably a good average is achieved by looking at the transaction ledger and finding the IP number of the device that has not had a token sent to it for the longest time.

[00049] Preferably the system thereby ensures that no individual device on a network is allowed to be ignored or excluded from regular transactions and also can be used to trigger an investigation as to why the device is no longer available on the network.

[00050] In yet a further broad form of the invention there is provided a method of verification of identity of network devices participating in a block chain; said Block chain comprising a plurality of ledgers held on a plurality of said network devices; said network devices communicating contents of the ledgers between them over a network; said devices verifying the contents of the ledgers as part of the step of communicating the contents of the ledgers; said method comprising

incorporating a unique identifier of a network device within the ledger maintained by the network device.

[00051] Preferably the network device stores a data record structure adapted for transmission over a network; the data record generated on the network device participating in a Blockchain as an initiating device which has an initiating device unique identifier; the data record structure containing at least a first record and a first unique identifier record; the first record containing data for transmission over the network to a device having a receiving device unique identifier; the first unique identifier record containing the initiating device unique identifier.

[00052] Preferably data from or pertaining to the first record is contained in a ledger.

[00053] Preferably the data record structure is contained within a wallet.

[00054] Preferably the data record structure further includes a second IP address record.

[00055] Preferably the second IP address record contains the receiving device IP address.

[00056] Preferably the data record structure further includes a second record.

[00057] Preferably the data record structure further includes a third record.

[00058] Preferably the first record contains token identifying data which uniquely identifies a token.

[00059] Preferably the token is exchanged between the initiating device and the receiving device.

[00060] Preferably the second record contains data which uniquely identifies a sending party.

[00061]

[00062] Preferably the third record contains data which uniquely identifies a receiving party.

[00063]

[00064] Preferably the data record structure further includes a hash range.

[00065]

[00066] In a further broad form there is provided a methodology to provide a predetermined level of confidence that a machine or network device in a block chain network is the machine or

network device you think it is. Token rotation keeps tokens current. If the token is rotated often enough then it is easy to see if a device has changed its unique identifier or has dropped off the network.

[00067]

[00068] In a further aspect we are combining both a user ID (preferably the public key) with a machine fingerprint within the ledger operating in a block chain environment so that it will be immediately detected if the machine fingerprint changes next time a token transfer session takes place with that machine.

[00069]

DRAWINGS

Embodiments of the present invention will now be described with reference to the accompanying drawings wherein:

[00070] Figure 1 illustrates the main components of an example embodiment

[00071] Figure 2 illustrates a transaction of the example embodiment

[00072] Figure 3 illustrates detail of a transaction of the example embodiment

[00073] Figure 4 illustrates the unique identifier verification process of the example embodiment

[00074] Figure 5 illustrates an automatic resend of token capability of the example embodiment.

[00075] Figure 6 is a block diagram of a system operating according to a further embodiment.

[00076] Figure 7 is a data structure diagram usable in accordance with blockchain protocol.

[00077] Figure 8 is a network diagram of devices participating in a blockchain.

[00078]

DESCRIPTION AND OPERATION

[00079] Figure 1 discloses the main components of the example embodiment. Each BlockChain network comprises multiple devices 10 11 12, each of which have and typically must have a unique IP address 13 14 15. For each device 10 11 12 to be part of a BlockChain network, each device 10 11 12 would typically have a wallet 16 that is accompanies by a public key 17 which is shared with the rest of the network for identification, encryption and decryption purposes, as well as a private key which is used for authentication encryption and decryption purposes.

[00080] The wallet 16 would also be accompanied by a BlockChain transaction record 19. Typically it 19 would not traditionally include the IP number of each sender and receiver of network tokens 21, however in the case of the example embodiment, the IP number of both sender 22 and receiver 23 in a transaction are included. All devices in the network 10 11 12 each have a wallet.

[00081] Figure 2 discloses an example transaction of the example embodiment. A wallet 30 receives 31 a token from another wallet on the network. The wallet 30 includes a public key 33 which is used for encryption and decryption as well as identification. The wallet 30 also has a private key 34 which is used for encryption, decryption and authentication. The wallet 30 also has an associated device IP address 35. The wallet 30 also has access to a transaction ledger 36 which uses block chain protocols to remain in sync with other ledgers 27 in the network.

[00082] When a token 32 is received by a wallet 30, the token 36 is then re routed to another wallet 39 which also has its own public key 40, private key 41 and associated ledger 37. This wallet is also associated with a device IP number 42.

[00083] When a token 36 is sent 38 from one wallet to another, information about the transaction is recorded in ledgers 36 37 including but not limited to the identity of the token 36, the identity of both the sending 33 and receiving wallets 40, and the time of the transaction.

[00084] In the case of the example embodiment, the IP numbers of both the sending 35 and receiving device 42 are also recorded in the transaction ledger 36 37. The benefit of this is that a history of ownership and integrity of association between the IP number and a secure wallet is established. This history of trust can be used to detect attempts to impersonate a device on a network.

[00085] If an intruder steals an IP number but does not have a legitimate secure wallet the impersonation can be easily detected.

[00086] The ledgers 36 37 use a system of digital signing that is known in the art as a means of tamper proofing the recorded information and verifying that the sender and receiver are who they say they are.

[00087] Figure 3 discloses details of a transaction of the example embodiment. A transaction record 50 typically contains information about the token being exchanged 51, information about the sending party 52 and the receiving party 53. However in the case of the example embodiment, the IP number of the sending device 54 and the IP address of the receiving device 55 are also included in the transaction record 50. This information is then hashed 56 using a process known in the art and digitally signed using a process that is known in the art.

[00088] This process of hashing and signing the transaction record, means that the record cannot be tampered with or changed in order to manipulate data in the record including but not limited to the IP address of the sending or receiving devices.

[00089] Figure 4 shows the IP verification process of the example embodiment. A device 60 referred to in a transaction file 62 typically has a unique IP address 61, which can be recorded as part 63 of a transaction file 62 which is then hashed and signed to maintain its integrity.

[00090] The fact that the recorded IP address and the IP of the device either sending or receiving tokens can be independently verified 64 means that the veracity of a device's IP address can be checked and verified and a decision made as to whether other parties can trust that device and its identity.

[00091] Figure 5 discloses the automatic resend of token capability of the example embodiment. When a wallet 72 receives 70 a token 71 from another wallet, a timer 73 and timing mechanism is set to automatically forward 74 the token 71 on to another device on the network 75. This is done to ensure that all devices on the network receive a regular delivery of tokens and helps to ensure that the transaction ledger remains current and active.

[00092] The wallet 72 also has built in rules 80 that are used to define if the wallet will receive or reject tokens 71 that are sent to it. For example, if the IP number of the device sending the token 70 does not exist in the transaction ledger 76 then reject the transaction. If the token identity is not known and not in the ledger then reject the token. Another example is when the IP recorded in the transaction record of the sending device does not match the IP of the device sending the token, then the token is rejected.

[00093] When the timing mechanism sends a token onto another device in the network, it would typically want to send the token to the network device that has not had a delivery of a token for the longest time top ensure that all devices on the network get a good average of transactions over time.

[00094] This can be achieved by looking at the transaction ledger 76 and finding the IP number of the device 79 that has not had a token sent to it for the longest time. This method ensures that no individual device on a network is allowed to be ignored or excluded from regular transactions and also can be used to trigger an investigation as to why the device is no longer available on the network.

FURTHER EMBODIMENT

[00095] With reference to figure 6 there is illustrated a system 200 in accordance with a further embodiment of the present invention providing additional security to a block chain system.
[00096]

[00097] In this instance the system includes at least a first node 201. In this instance the node 201 comprises a network device in the form of a server having at least a memory 202, a processor 203 and an input/output device 204 operable to communicate over a network 205 with at least a second node 206. In this instance the second node 206 also comprises a network device in the form of the server comprising at least memory 207 in communication with processor 208 which, in turn, is in communication with input output device 209. In alternative forms the network device may comprise a router. In alternative forms it may comprise any intelligent device which is network connected and has sufficient processing power to perform the functions outlined for this embodiment.

[00098] The system 200 operates in a block chain environment in accordance with Block chain protocols and includes the transmission and retention of data and related meta data in a ledger structure 210. Additional details of at least generalised forms of Block chain protocols and utilisation of the ledger structure are given further below with reference to figures 7 and 8.

[00099] In use the system 200 includes information stored in a wallet 211 within memory 202. Fields in the wallet, in this instance, include a token field 212, a public key field 213, a private key field 214 and a device identifier field 215. Corresponding fields are structured into the wallet 216 of second node 206 and, indeed, into any other device operating within the block chain of

system 200.

[000100] In use, in one form the wallet 211 contains a unique identifier for device 201 in its identifier field 215. In a preferred form the unique identifier is the IP address of the device 201. In alternative forms it may be the MAC address of the device 201. In yet other forms it may be related to the hardware comprising the device 201.

[000101]

[000102] As part of the transmission of a token A over network 205 from first wallet 211 to second wallet 216 various items of information in the form of data are stored in the ledger as generally illustrated in figure 6. These include the identity of the first wallet -in a preferred form being the public key of the first wallet 211 stored in record 213. Also stored in the ledger 210 will be the unique identifier of the device 201 which houses the wallet 211-in this specific instance the IP address of the device 201. The ledger 210 is subject to steps to assist in its verification in accordance with Block chain protocols. In one form this can include applying a hash algorithm to the data in the ledger. In a further form this may additionally include digitally signing the resulting hash of the data. This step allows comparison to be made against the data in the ledger at subsequent times, preferably at the times when a token is either transmitted to or from the wallet whereby if the unique identifier of the device 201 which houses the wallet 211 changes this will be detected-for example by detecting that the hash value has changed.

[000103] In preferred forms the token A is transmitted from device to device on the network on a rotating basis to ensure that every device receives or sends the token A over a predetermined period of time thereby to test the integrity/identity of each device on the network that is participating in the block chain.

[000104] You will be noted that this testing of integrity/identity of device 201 will occur in effect automatically as part of the normal following of the block chain protocol by virtue of inclusion of the device identifier within the ledger 210.

[000105] In a preferred form the token A may simply comprise an alphanumeric sequence whose primary purpose is to be sent from device to device thereby to trigger tests of device identity by way of ledger verification that takes place as part of the block chain protocol. In other forms the token A may have a representative value-for example it may represent an element of bit coin value – for example 1 Satoshi in Bitcoin value.

[000106] In yet other forms the token A may be an element of data that is desired to be transmitted from one wallet to another for reasons associated with the intrinsic nature of the data as a unit of currency or as a unit of information.

[000107] A byproduct of this routine checking of identity is that as the number of transactions on a particular network device rises there is an inference of reliability of that network device and its

identity. Conversely where a network device has changed its unique identifier then a decision may be made not to send data to the wallet on that machine for at least a predetermined period of time.

[000108] Broadly the idea is to provide a certain level of confidence that a machine or network device in the block chain network is the machine or network device you think it is. Token rotation keeps tokens current. If the token is rotated often enough then it is easy to see if a device has changed its unique identifier or has dropped off the network.

[000109]

[000110] In one aspect we are combining both a user ID (preferably the public key) with a machine fingerprint within the ledger operating in a block chain environment so that it will be immediately detected if the machine fingerprint changes next time a token transfer session takes place with that machine.

[000111] In another aspect the above described methodology provides a method of introduction of a new network device or machine onto a network.

[000112] This methodology can be given effect by designating a mother wallet or initiating wallet which allocates/sends out new tokens to a new network device.

[000113] The new network device has to build a wallet then the mother wallet sends a first token to it thereby to initiate the machine/network device onto the block chain network of which it is to become a trusted part.

[000114]

BLOCK CHAIN STRUCTURES

[000115] Blockchain structures as described elsewhere in this specification and below are used with any of the above described embodiments.

[000116] Figure 7 is a diagram of an exemplary block chain data structure.

[000117] Figure 8 illustrates diagrammatically use of the block chain data structure of figure 7.

[000118] With reference to figures 7 and 8, Blockchain is a data structure and distributed record system which seeks to provide a data structure and system which in preferred forms maintains a complete record of all transactions and minimizes risk of retrospective alterations, or double or identical transactions.

[000119] The data structure consists of a series of transactions grouped in blocks, which need to be verified before they are added to the chain. Rules may be set so no data is ever deleted, with the longest chain being taken to be the most recent, and so the chain records all transactions from its initiation in chronological order.

[000120] A copy of the chain may be kept by all users, and so is a distributed record system. Before any transactions are added the majority of the users need to agree that the transaction is acceptable and then it is bundled with other acceptable transactions into a block, which is added to the chain. Each block has a header which can only be created knowing all the previous transactions. As a result, if a retrospective alteration is made the header will be incorrect and any new block proposed by that user will be rejected. The security of the system is further enhanced by having mathematical problems that can only be solved by trial and error, which use the header and must be solved and then verified by the majority of other users before a block is accepted into the chain by all users. As long as there are more genuine users than coordinated attackers trying to alter the chain then the chain will be secure. There may be other methods used to determine the veracity of a block of data, this may include voting or consent processes where parties with a stake in the transaction or related transactions or in the chain itself are granted 'voting' rights. Another process may involve a random or systematized voting or approval system where the validity of the block of data is approved in accordance with a set of protocols agreed by those with a stake in the veracity of the chain of data.

[000121] In a more particular form, each block includes verified transactions and the blockchain maintains a ledger all prior transactions. The blockchain is duplicated by all the computers on a network.

[000122] The first block in the chain is known as the Genesis block and new blocks can be added in linear and chronological order. From any given block in the chain the information of this genesis block and all blocks that led back to this one can be retrieved. A blockchain is essentially numerous blocks connected through hash chaining where each block is comprised of the following

- Timestamp: provides proof that the data in a block existed at a particular time
- Previous Hash: Essentially a pointer to the previous block
- Merkle Hash: Summary of all executed transactions
- Nonce: Individual blocks identity and is an arbitrary number which can only be used once

[000123] The blockchain is managed by a network of distributed nodes where each node contains a copy of the entire blockchain. Each node in the network can add blocks to the chain, where every node is adding blocks at the same point in the chain at the same time. The more nodes that comprise the network the harder it is to disrupt the storage of the blockchain. Unlike centralised systems which rely on a single authority, there is no single point of failure in these distributed nodes network. If you change the content of a block you change its Hash.

ALTERNATIVE EMBODIMENTS

[000124] The rules mentioned with reference to figure 5 are examples. An alternative embodiment may use any set of rules to govern the acceptance, rejection of tokens and the control of the wallet.

[000125] The example embodiment uses a device IP as an identifier of the device sending or receiving tokens. An alternative embodiment may use any externally verifiable information that can uniquely identify a device and be verified by a second party. Examples include a Mac address of a device or serial numbers of component parts of the device. Preferably the identifier is not able to be modified easily or at all by a second party without security clearance. Additionally the external unique identifier would be included in the transaction record and also included in the hash calculation and digital signing by the sending or receiving party or parties.

[000126] The example embodiment shows only a few devices in the network for simplicity. An alternative embodiment may have any number of devices in the network.

[000127] The example embodiment uses the standard hashing and digital signing methodologies commonly used in BlockChain networks. An alternative embodiment may use any method of integrity, authentication and identification methods available.

[000128] The example embodiment uses a timing rule as a means of triggering when a token that is received is resent to another device on the network. An alternative embodiment could use any triggering calculation or method to ensure that tokens are circulated at a regular interval amongst the devices on the shared network. Parameters such as network congestion and the ideal level of security through regular identity verification can be factors that can be included in the calculation of how regularly each wallet shares tokens amongst the other computers in the network.

CLAIMS

1. A data record structure adapted for transmission over a network; the data record generated on a network device participating in a Blockchain as an initiating device which has an initiating device unique identifier; the data record structure containing at least a first record and a first unique identifier record; the first record containing data for transmission over the network to a device having a receiving device unique identifier; the first unique identifier record containing the initiating device unique identifier.

2. The data record of claim 1 wherein data from or pertaining to the first record is contained in a ledger.

3. The data record structure of claim 1 wherein the data record structure is contained within a wallet.

4. The data record structure of claim 1 or claim 2 wherein the data record structure further includes a second IP address record.

5. The data record structure of claim 3 wherein the second IP address record contains the receiving device IP address.

6. The structure of any one of claims 1 to 4 wherein the data record structure further includes a second record.

7. The structure of any one of claims 1 to 5 wherein the data record structure further includes a third record.

8. The structure of any previous claim wherein the first record contains token identifying data which uniquely identifies a token.

9. The structure of claim 7 wherein the token is being exchanged between the initiating device and the receiving device.

10. The structure of any previous claim wherein the second record contains data which uniquely identifies a sending party.

11. The structure of any previous claim wherein the third record contains data which uniquely identifies a receiving party.

12. The structure of any previous claim wherein the data record structure further includes a hash range.

13. A transmission system for transmission of the data record structure of any one of claims 1 to 12.

14. The system of claim 12 wherein the data record structure is stored on an intermediate database as an intermediate database record.

15. The system of claim 13 wherein a hash of the data record structure is stored on the intermediate database as part of the intermediate database record.

16. The system of claim 12, 13 or 14 wherein the intermediate database record is stored on a plurality of intermediate databases; each intermediate database separate and distinct from any other of the plurality of intermediate databases.

17. The system of claim 15 wherein the plurality of intermediate databases form part of a BlockChain network.

18. The system of claim 15 wherein the data record structure is accompanied by a public key which is shared with the rest of the network for identification, encryption and decryption purposes.

19. The system of claim 17 wherein the data record structure includes a private key which is used for authentication, encryption and decryption purposes.

20. The system of any one of claims 12 to 18 wherein the wallet also has access to a transaction ledger which uses block chain protocols to remain in sync with other ledgers in the network.

21. The system of claim 19 wherein when a token is received by a wallet, the token is then re routed to another wallet which also has its own public key, private key and associated ledger.

22. The system of claim 19 or 20 wherein when a token is sent from one wallet to another, information about the transaction is recorded in ledgers including but not limited to the identity

of the token, the identity of both the sending and receiving wallets, and the time of the transaction.

23. The system of claim 19, 20 or 21 wherein the IP numbers of both the sending and receiving device are also recorded in the transaction ledger thereby to establish and maintain a history of ownership and integrity of association between the IP number and a secure wallet.

24. The system of claim 22 wherein the history of trust can be used to detect attempts to impersonate a device on the network.

25. The system of any one of claims 12 to 23 incorporating an automatic resend capability.

26. The system of claim 24 wherein when a wallet receives a token from another wallet, a timer and timing mechanism is set to automatically forward the token on to another device on the network.

27. The system of claim 25 wherein the timing mechanism ensures that all devices on the network receive a regular delivery of tokens and helps to ensure that the transaction ledger remains current and active.

28. The system of any one of claims 12 to 26 wherein the wallet also has built in rules that are used to define if the wallet will receive or reject tokens that are sent to it.

29. The system of claim 27 wherein if the IP number of the device sending the token does not exist in the transaction ledger then reject the transaction.

30. The system of claim 27 wherein if the token identity is not known and not in the ledger then reject the token.

31. The system of claim 27, 28 or 29 wherein if the IP address recorded in the transaction record of the sending device does not match the IP address of the device sending the token, then the token is rejected.

32. The system of any one of claims 25 to 30 wherein when the timing mechanism sends a token on to another device in the network, the system is programmed to send the token to the network device that has not had a delivery of a token for the longest time thereby to ensure

that all devices on the network get a good average of transactions over time.

33. The system of claim 31 wherein a good average is achieved by looking at the transaction ledger and finding the IP number of the device that has not had a token sent to it for the longest time.

34. The system of claim 32 which thereby ensures that no individual device on a network is allowed to be ignored or excluded from regular transactions and also can be used to trigger an investigation as to why the device is no longer available on the network.

35. A method of verification of identity of devices participating in a block chain; said Block chain comprising a plurality of ledgers held on a plurality of network devices; said network devices communicating contents of the ledgers between them over a network; said devices verifying the contents of the ledgers as part of the step of communicating the contents of the ledgers; said method comprising incorporating a unique identifier of a network device within the ledger maintained by the network device.

36. The method of claim 35 wherein the network device stores a data record structure adapted for transmission over a network; the data record generated on the network device participating in a Blockchain as an initiating device which has an initiating device unique identifier; the data record structure containing at least a first record and a first unique identifier record; the first record containing data for transmission over the network to a device having a receiving device unique identifier; the first unique identifier record containing the initiating device unique identifier.

37. The method of claim 35 wherein data from or pertaining to the first record is contained in a ledger.

38. The method of claim 35 or claim 36 wherein the data record structure is contained within a wallet.

39. The method of claim 35 or claim 36 wherein the data record structure further includes a second IP address record.

40. The method of claim 35 or claim 36 wherein the second IP address record contains the receiving device IP address.

41. The method of claim 35 or claim 36 wherein the data record structure further includes a second record.

42. The method of claim 35 or claim 36 wherein the data record structure further includes a third record.

43. The method of claim 35 or claim 36 wherein the first record contains token identifying data which uniquely identifies a token.

44. The method of claim 35 or claim 36 wherein the token is being exchanged between the initiating device and the receiving device.

45. The method of claim 35 or claim 36 wherein the second record contains data which uniquely identifies a sending party.

46. The method of claim 35 or claim 36 wherein the third record contains data which uniquely identifies a receiving party.

47. The method of claim 35 or claim 36 wherein the data record structure further includes a hash range.

48. A non-transitory computer readable medium having computer executable instructions stored thereon which when executed by a processor perform the method of any one of claims 35 to 47.

49. A network device including at least a processor, a memory and an input output device which executes the method of any one of claims 35 to 47.

50. A method for providing a level of trust in a machine or network device in a block chain network; the method comprising
including both a user identifier and a unique identifier of a machine or network device within the ledger associated with that machine or network device operating in a block chain environment whereby it will be immediately detected if the machine fingerprint changes next time a token transfer session takes place with that machine.

51. The method of claim 50 wherein the user identifier is the public key accorded the user of the machine.

52. The method of claim 50 or 51 wherein the unique identifier of the machine or network device is a machine fingerprint.

53. The method of claim 52 wherein the machine fingerprint comprises a hardware characteristic of the machine or network device.

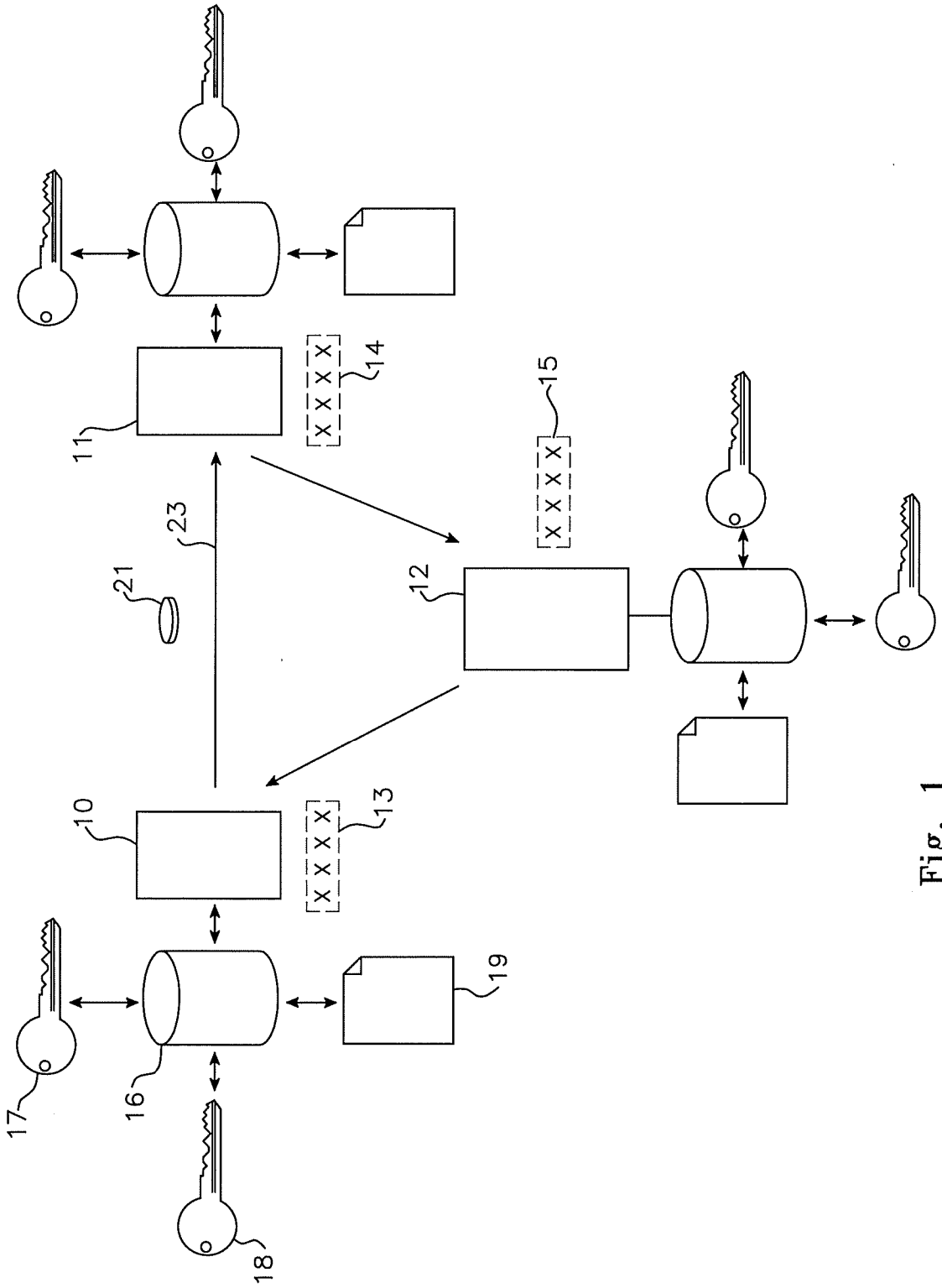

Fig. 1

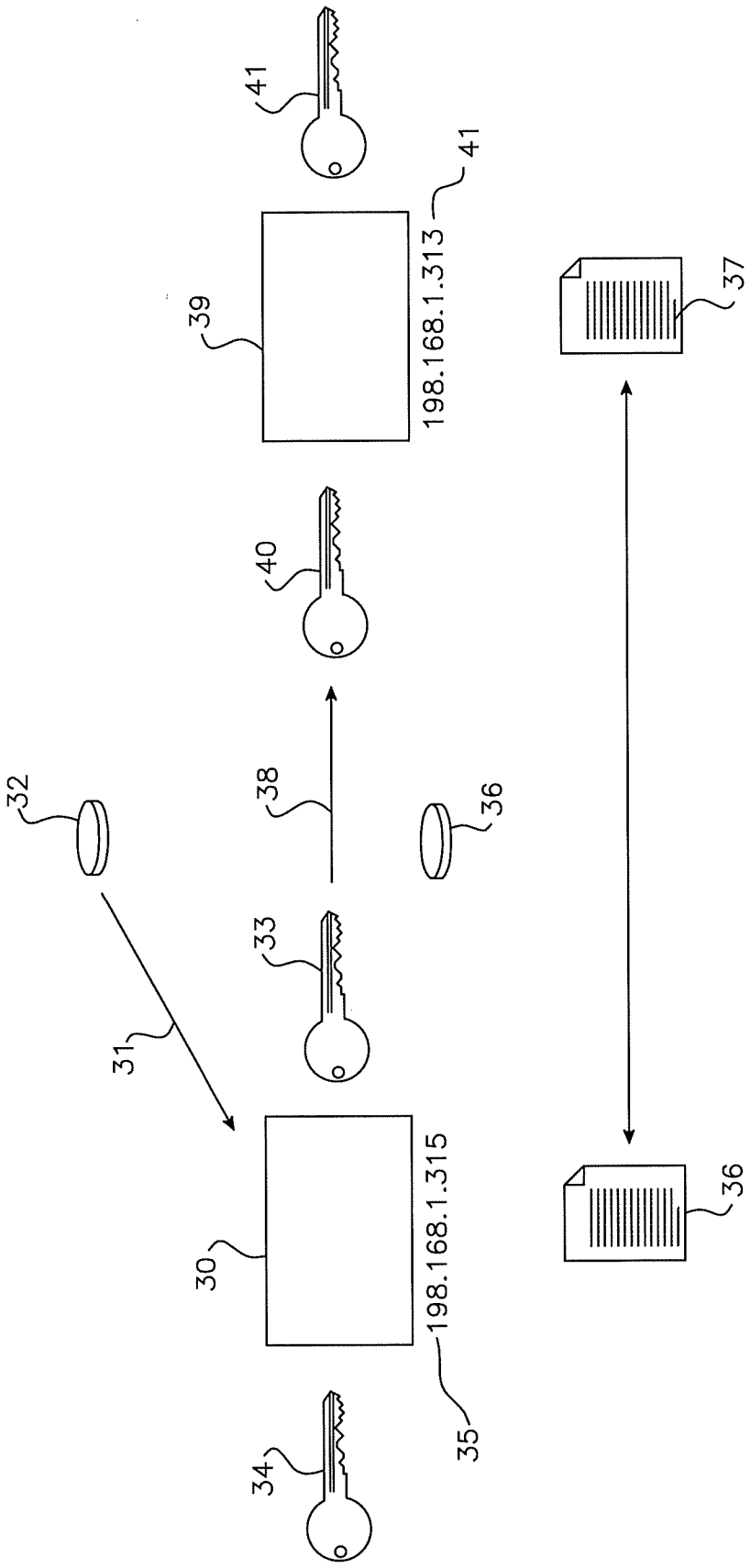

Fig. 2

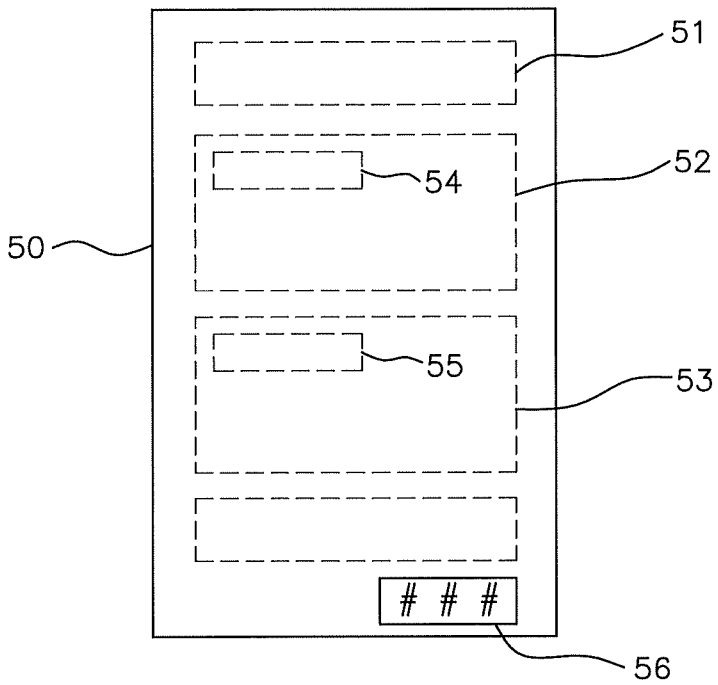

Fig. 3

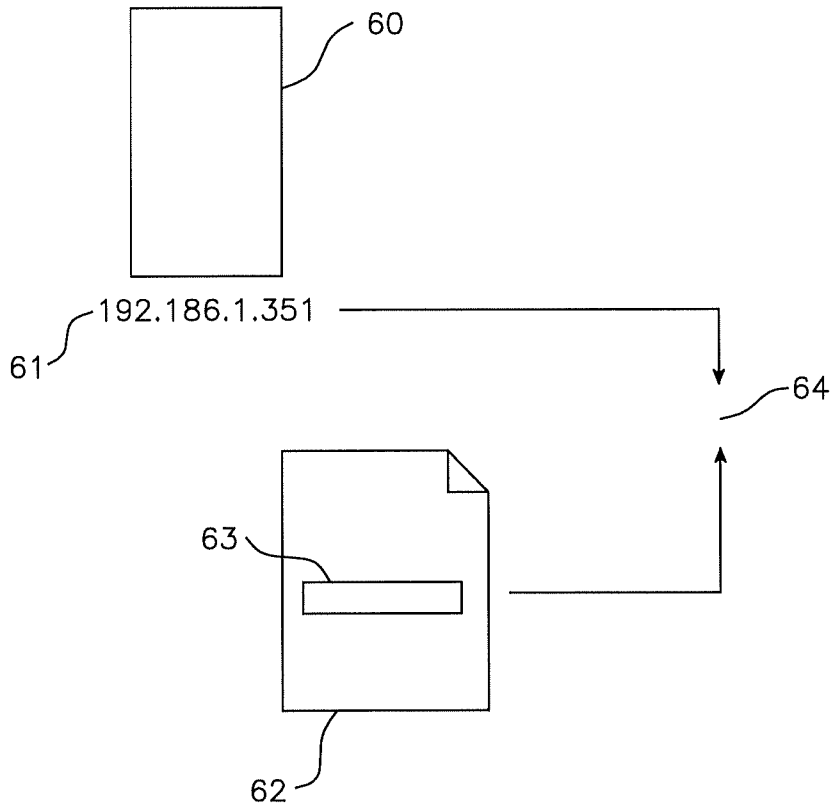

Fig. 4

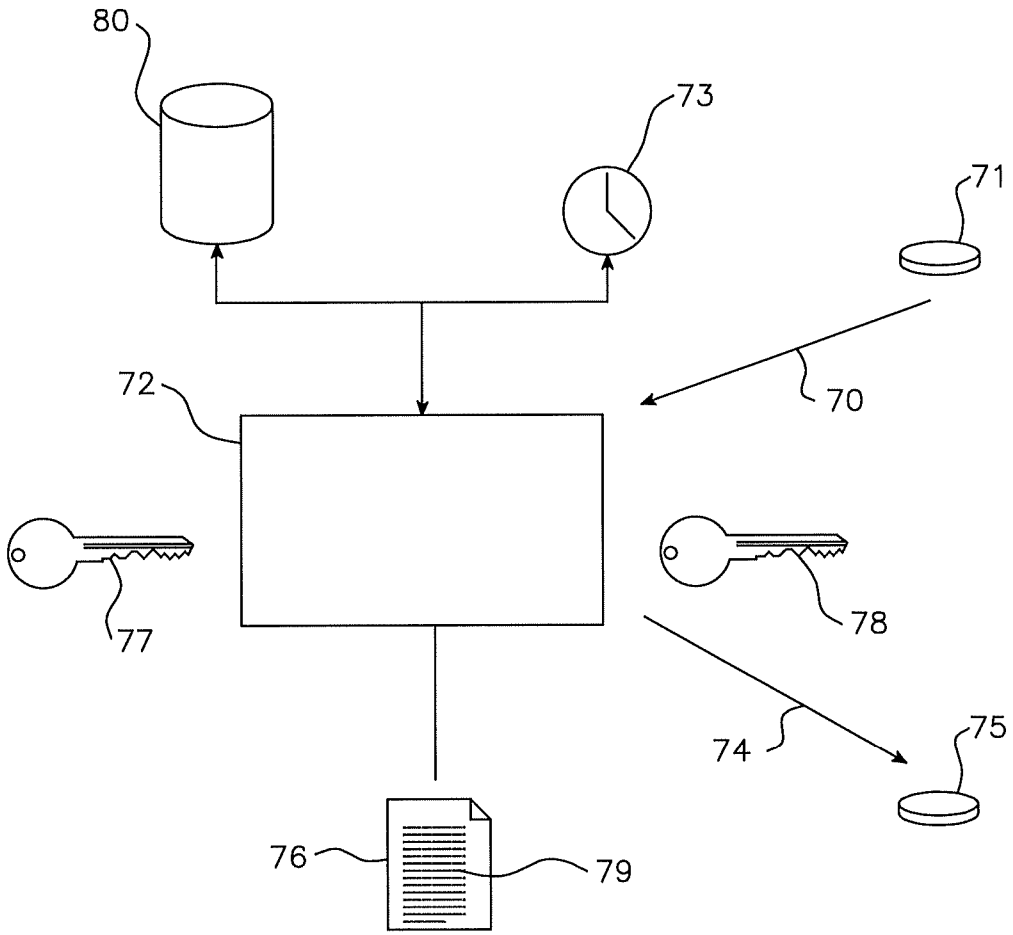

Fig. 5

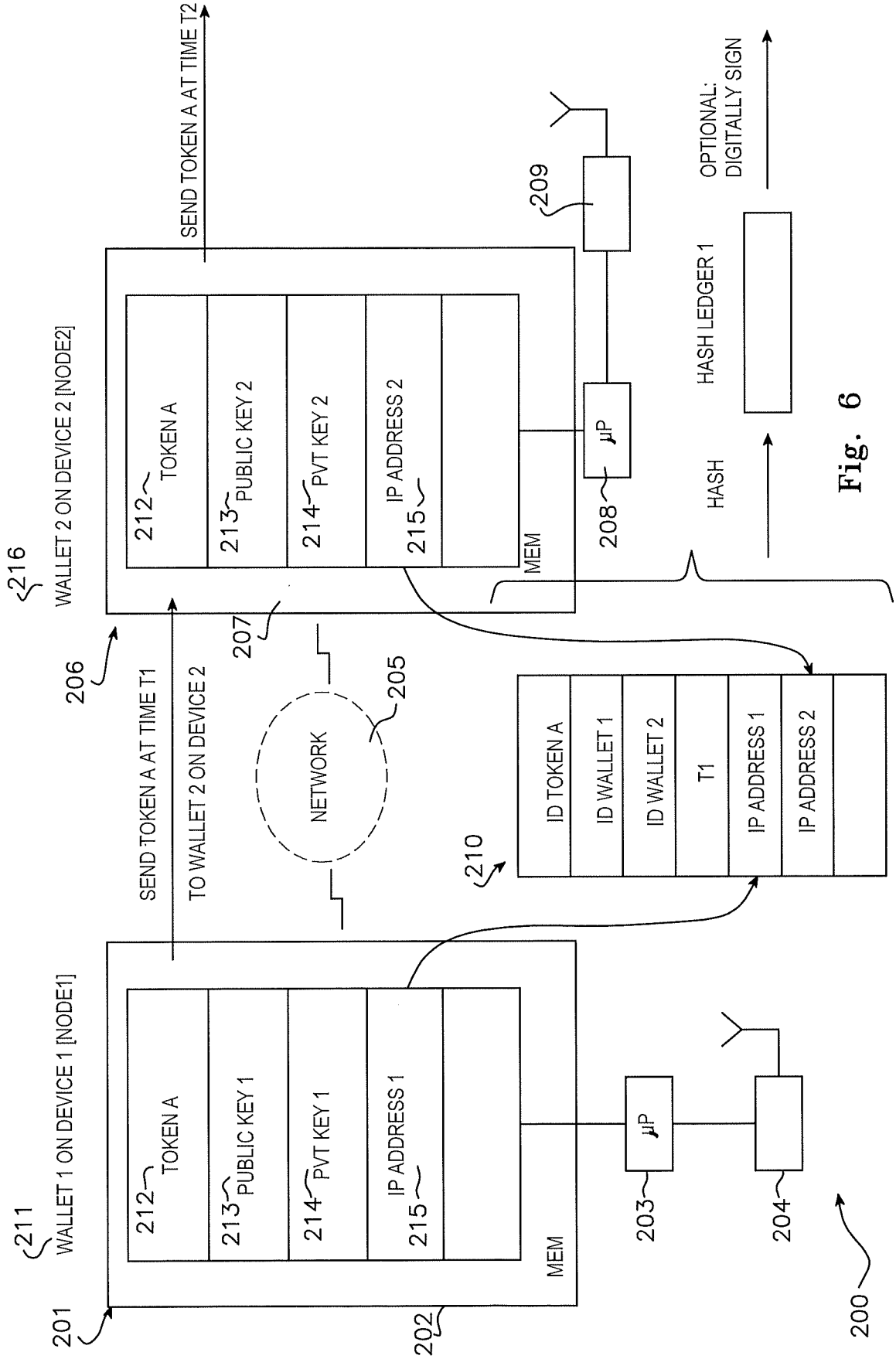
SEND TOKEN A AT TIME T2
OPTIONAL: DIGITALLY SIGN
HASH LEDGER 1
HASH
209
216
WALLET 2 ON DEVICE 2 [NODE2]
212 TOKEN A
213 PUBLIC KEY 2
214 PVT KEY 2
215 IP ADDRESS 2
MEM
208 µP
206
207
SEND TOKEN A AT TIME T1
TO WALLET 2 ON DEVICE 2
NETWORK
205
ID TOKEN A
ID WALLET 1
ID WALLET 2
T1
IP ADDRESS 1
IP ADDRESS 2
210
211
WALLET 1 ON DEVICE 1 [NODE1]
212 TOKEN A
213 PUBLIC KEY 1
214 PVT KEY 1
215 IP ADDRESS 1
MEM
203 µP
204
201
202
200

Fig. 6

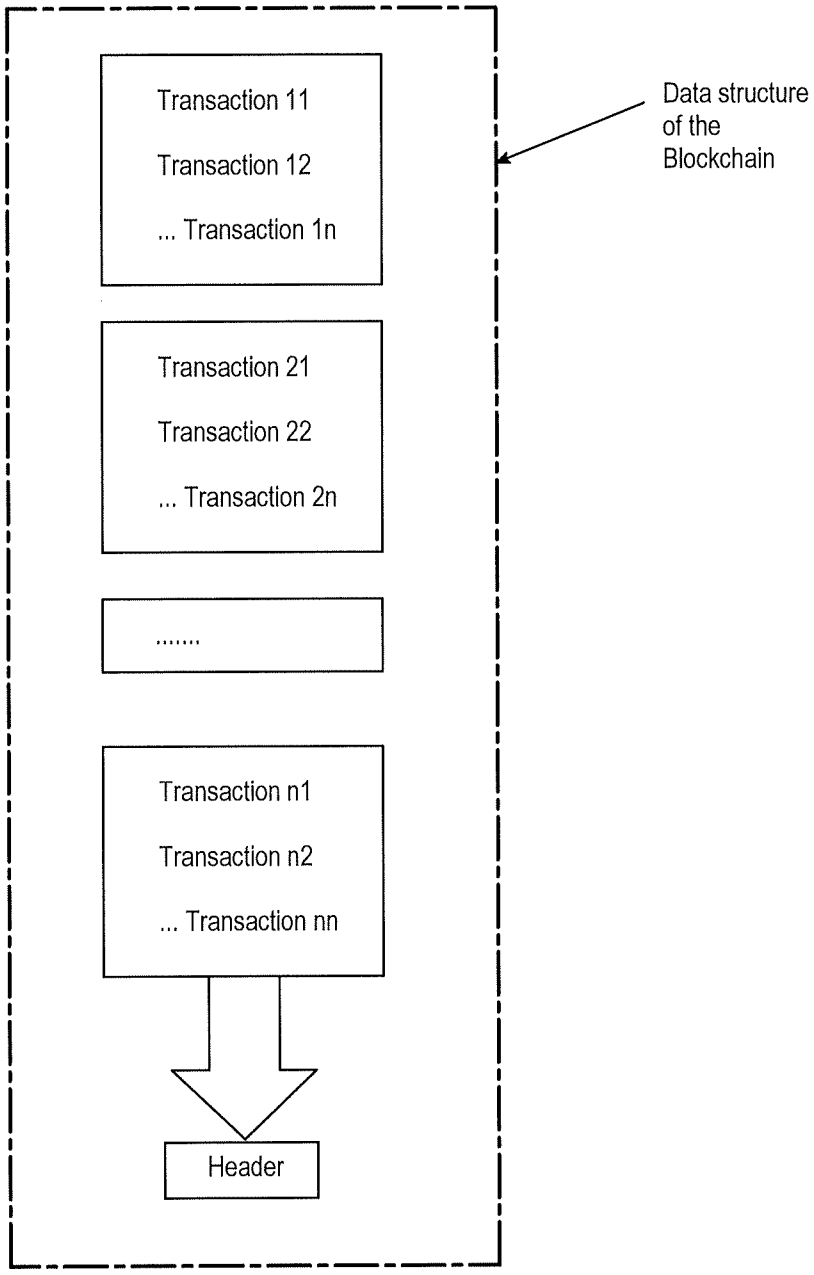
Transaction 11
Transaction 12
... Transaction 1n
Transaction 21
Transaction 22
... Transaction 2n
.....
Transaction n1
Transaction n2
... Transaction nn
Header
Data structure of the Blockchain

Fig. 7

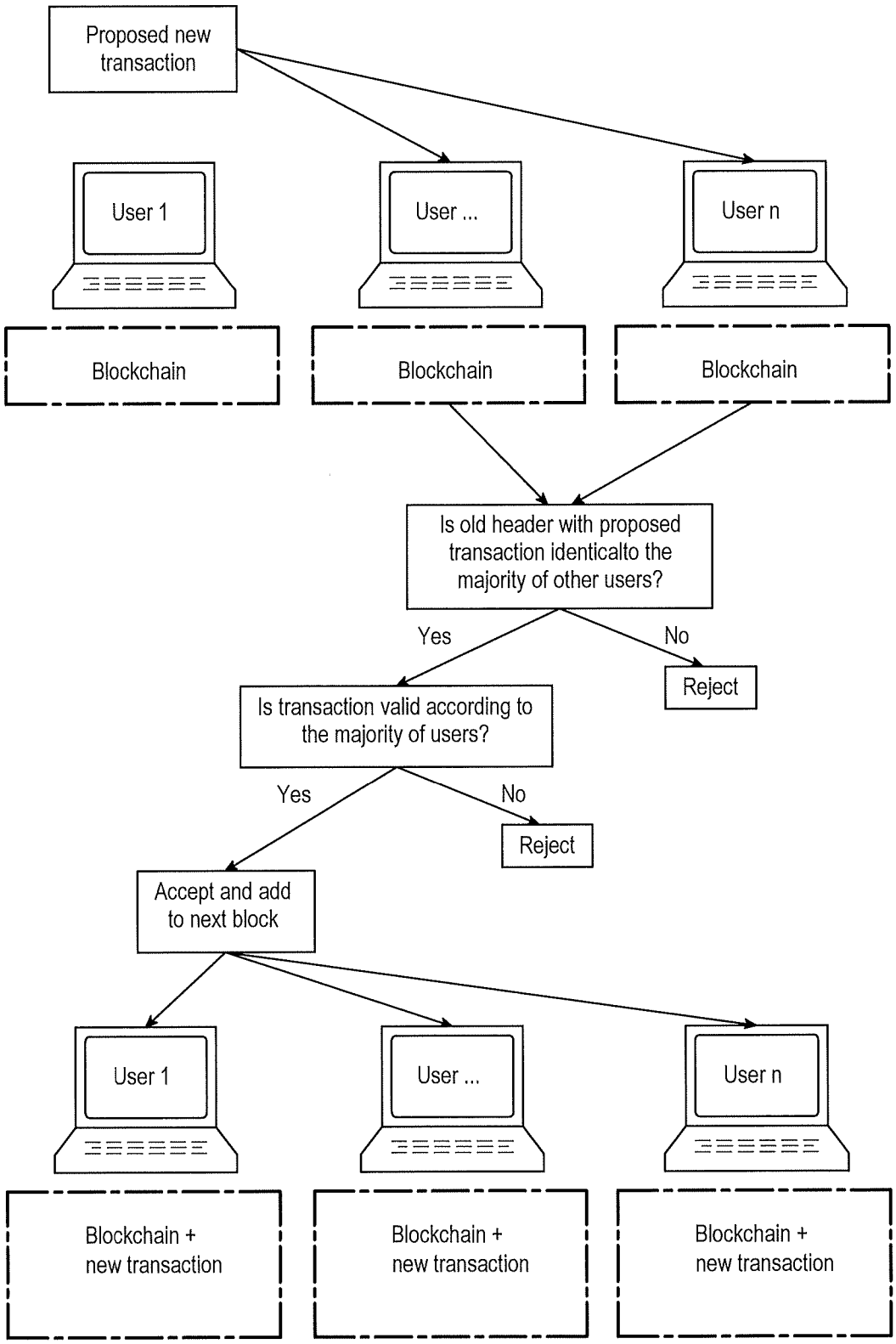
Proposed new transaction
User 1
User ...
User n
Blockchain
Blockchain
Blockchain
Is old header with proposed transaction identicalto the majority of other users?
Yes
No
Reject
Is transaction valid according to the majority of users?
Yes
No
Reject
Accept and add to next block
User 1
User ...
User n
Blockchain + new transaction
Blockchain + new transaction
Blockchain + new transaction

Fig. 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2017/000090

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/40 (2012.01)

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

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)

EPODOC, WPIAP: Keywords used (blockchain, ledger, wallet, MAC, fingerprint, change) and similar terms

Google, Google Patents, Google Scholar: Keywords used (blockchain, ledger, wallet, MAC, fingerprint, change) and similar terms

Google, Google Patents, Google Scholar and IP Australia Internal Databases: Applicant/Inventor name search

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	Documents are listed in the continuation of Box C	

[X] 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	Date of mailing of the international search report
21 July 2017	21 July 2017
Name and mailing address of the ISA/AU	**Authorised officer**
AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA Email address: pct@ipaustralia.gov.au	Kanwal Pahwa AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No. +61262837922

INTERNATIONAL SEARCH REPORT C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		International application No. **PCT/AU2017/000090**
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	GREENSPAN G "Multichain Private Blockchain - White Paper" <http://web.archive.org/web/20160403063334/http://www.multichain.com/download/MultiChain-White-Paper.pdf >, retrieved from Internet, published on 3 April 2016 as per wayback engine Pages 1-17 Pages 1, 2, 5, 6, 8-9, 10, 12, 14-15, 23-24	1-49
X Y	US 2015/0206106 A1 (YARON EDAN YAGO) 23 July 2015 Fig 4, Para 0065, 0075, 0077, Para 0077	1-2, 4-7, 10-19, 35-37, 39-42, 45-49 50-53
Y	US 2016/0071108 A1 (IDM GLOBAL INC) 10 March 2016 Para 0047	50-53
A	KR 100749247 B1 (LG TELECOM LTD) 07 August 2007 Abstract	50-53
P,X	WO 2016/156954 A1 (BLACK GOLD COIN INC) 06 October 2016 Pg 6-9, 16, 23-24	1-49

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2017/000090

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:
the subject matter listed in Rule 39 on which, under Article 17(2)(a)(i), an international search is not required to be carried out, including

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a)

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

See Supplemental Box for Details

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☒ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

Supplemental Box

Continuation of: **Box III**

This International Application does not comply with the requirements of unity of invention because it does not relate to one invention or to a group of inventions so linked as to form a single general inventive concept.

This Authority has found that there are different inventions based on the following features that separate the claims into distinct groups:

- Claims 1-49 are directed to a data record structure for transmission over a network.. The feature of the means to record structure containing at least a first record and a first unique identifier record and the first record containing data for transmission over the network to a device having a receiving device unique identifier is specific to this group of claims.

- Claims 50-53 are directed to a method of providing a level of trust in block chain network.. The feature of the means to include user identifier and unique identifier within the ledger and immediately detecting if the machine fingerprint changes is specific to this group of claims.

PCT Rule 13.2, first sentence, states that unity of invention is only fulfilled when there is a technical relationship among the claimed inventions involving one or more of the same or corresponding special technical features. PCT Rule 13.2, second sentence, defines a special technical feature as a feature which makes a contribution over the prior art.

When there is no special technical feature common to all the claimed inventions there is no unity of invention.

In the above groups of claims, the identified features may have the potential to make a contribution over the prior art but are not common to all the claimed inventions and therefore cannot provide the required technical relationship. Therefore there is no special technical feature common to all the claimed inventions and the requirements for unity of invention are consequently not satisfied *a priori*.

INTERNATIONAL SEARCH REPORT Information on patent family members	International application No. **PCT/AU2017/000090**

This Annex lists known patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document/s Cited in Search Report		**Patent Family Member/s**	
Publication Number	**Publication Date**	**Publication Number**	**Publication Date**
US 2015/0206106 A1	23 July 2015	US 2015206106 A1	23 Jul 2015
		WO 2015106285 A1	16 Jul 2015
US 2016/0071108 A1	10 March 2016	US 2016071108 A1	10 Mar 2016
		US 2010293094 A1	18 Nov 2010
		US 9471920 B2	18 Oct 2016
		US 2015324802 A1	12 Nov 2015
		US 2016063500 A1	03 Mar 2016
		US 2016371693 A1	22 Dec 2016
		US 2017140386 A1	18 May 2017
KR 100749247 B1	07 August 2007	KR 100749247 B1	07 Aug 2007
WO 2016/156954 A1	06 October 2016	WO 2016156954 A1	06 Oct 2016
		EP 3073670 A1	28 Sep 2016
		US 2016283941 A1	29 Sep 2016

End of Annex

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.