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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 September 2017 (28.09.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/162904 A1

(51) International Patent Classification:
H04L 9/08 (2006.01) *G06Q 20/22* (2012.01)
H04L 29/06 (2006.01) *G06Q 20/36* (2012.01)
G06F 21/64 (2013.01) *G06Q 20/38* (2012.01)

(21) International Application Number:
PCT/FI2016/050187

(22) International Filing Date:
23 March 2016 (23.03.2016)

(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). **LI, Hongwei**; 42 Green End Road, Cambridge CB4 1RY (GB). **MARTIN LÒPEZ, 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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK,

[Continued on next page]

(54) Title: MANAGEMENT OF CRYPTOGRAPHIC TRANSACTIONS

(57) Abstract: According to an example aspect of the present invention, there is provided 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 configured to, with the at least one processing core, cause the apparatus at least to compile a set of transactions in a block chain based resource management system that have taken place after the most recent block was established, establish a new block in the block chain, and in establishing the new block, for transactions associated with verification accept messages and lacking sufficient resources, cause transferring of the lacking resources from verification nodes having sent the verification accept messages.

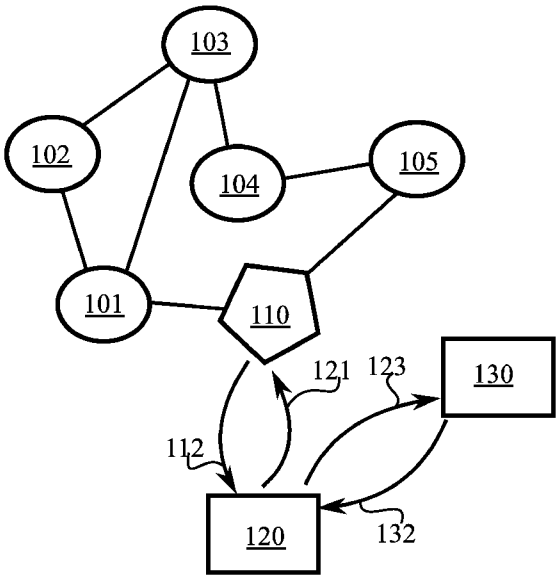

FIGURE 1

WO 2017/162904 A1

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))*

MANAGEMENT OF CRYPTOGRAPHIC TRANSACTIONS

FIELD

[0001] The present application relates to the field of managing cryptographic transactions.

BACKGROUND

[0002] Transactions in digital systems may take several different forms. For example, credit card transactions may be verified by querying, from an issuer of the card, whether a credit account associated with the credit card has sufficient remaining credit to cover the transaction. Additionally, a client identity may be verified, which may take place by requesting the client to enter a pin code or to provide a signature. In some cases, the client may be requested to present a proof-of-identity document, such as a passport. Yet further, a bank issuing the credit card may call the client's mobile phone before approving the transaction, in case the transaction meets certain criteria.

[0003] Where the digital system is not centrally managed, verifying a transaction may take place by requiring a proof-of-work from the client before agreeing to the verification. For example, before accepting a transaction, a computer system may issue a challenge to the client. The challenge may comprise a mathematical challenge, such as a partial hash function reversal, which the client can perform and the performance of which requires a moderate investment in processor cycles, for example. For example, the challenge may be computationally simple for the verifier to generate and to verify an answer the client provides is correct, but computationally more challenging for the client to perform to obtain the answer.

[0004] A further verification method is a block chain, wherein a resource is recorded in a ledger, which may be public. Changes in resource ownership take the form of transactions, wherein 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. A cryptographic signature may be generated using a private key of a private key-public key

pair. Validity of the cryptographic signature may be verified using the public key, while the signature can only be generated using the private key. While the public key may be freely shared with no reduction in security, the private key is closely kept by the owner.

[0005] In a block chain, transactions are recorded in blocks comprised in the chain, wherein the chain may comprise a distributed database. In principle, a chain of previous owners, or at least their identifiers, of each resource can be assessed based on the block chain.

SUMMARY OF THE INVENTION

[0006] The invention is defined by the features of the independent claims. Some specific embodiments are defined in the dependent claims.

[0007] According to a first aspect of the present invention, there is provided an apparatus comprising memory configured to store a block chain segment of a block chain based resource management system, and at least one processing core configured to process, based at least partly on the block chain segment, a verification request concerning a transaction, and to cause transmission of a verification accept message in response to the processing indicating the transaction is acceptable, before a new block is established in the block chain.

[0008] Various embodiments of the first aspect may comprise at least one feature from the following bulleted list:

- at least one processing core is configured to process the verification request at least partly by determining, whether a cryptographic signature comprised in the verification request is associated with sufficient resources to perform the transaction
- the at least one processing core is configured to process the verification request at least partly by determining, whether resources of a verification node would be transferred in the transaction

- the apparatus comprises a verification node, and the at least one processing core is configured to process the verification request at least partly in collaboration with other verification nodes
- the collaboration comprises transmitting the verification request to the other verification nodes
- the collaboration comprises requesting further block chain segments from the other verification nodes
- the verification accept message comprises a cryptographic signature of the apparatus
- the apparatus is configured to transmit the verification accept message to the node that sent the verification request message to the apparatus
- the apparatus is configured to transmit the verification accept message to at least one further verification node.

[0009] According to a second aspect of the present invention, there is provided 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 configured to, with the at least one processing core, cause the apparatus at least to: receive a new transaction in a block chain based resource management system cause transmission, to a verification node, of a verification request concerning the transaction, and transmit the transaction to a network responsive to a verification accept message from the verification node, before a new block is established in the block chain.

[0010] According to a third aspect of the present invention, there is provided 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 configured to, with the at least one processing core, cause the apparatus at least to compile a set of transactions in a block chain based resource management system that have taken place after the most recent block was established, establish a new block in the block chain, and in establishing the new block, for transactions associated with verification accept messages and lacking sufficient resources, cause transferring of the lacking resources from verification nodes having sent the verification accept messages.

[0011] Various embodiments of the third aspect may comprise the feature wherein the at least one memory and the computer program code are configured to, with the at least

one processing core, cause the transferring of the lacking resources by including, for each transaction associated with a verification accept message and lacking sufficient resources, in the new block, a transaction that transfers resources from the verification node that sent the associated verification message to a recipient of the transaction lacking sufficient resources.

[0012] According to a fourth aspect of the present invention, there is provided a method comprising storing, in an apparatus, a block chain segment of a block chain based resource management system, processing, based at least partly on the block chain segment, a verification request concerning a transaction, and causing transmission of a verification accept message in response to the processing indicating the transaction is acceptable, before a new block is established in the block chain.

[0013] Various embodiments of the fourth aspect may comprise at least one feature corresponding to a feature on the preceding bulleted list laid out in connection with the first aspect.

[0014] According to a fifth aspect of the present invention, there is provided a method, comprising receiving a new transaction in a block chain based resource management system, causing transmission, to a verification node, of a verification request concerning the transaction, and transmitting the transaction to a network responsive to a verification accept message from the verification node, before a new block is established in the block chain.

[0015] According to a sixth aspect of the present invention, there is provided a method, comprising: compiling a set of transactions in a block chain based resource management system that have taken place after the most recent block was established, establishing a new block in the block chain, and in establishing the new block, for transactions associated with verification accept messages and lacking sufficient resources, causing transferring of the lacking resources from verification nodes having sent the verification accept messages.

[0016] Various embodiments of the sixth aspect may comprise the feature wherein causing the transferring of the lacking resources comprises including, for each transaction associated with a verification accept message and lacking sufficient resources, in the new block, a transaction that transfers resources from the verification node that sent the

associated verification message to a recipient of the transaction lacking sufficient resources.

[0017] According to a seventh aspect of the present invention, there is provided an apparatus comprising means for storing a block chain segment of a block chain based resource management system, means for processing, based at least partly on the block chain segment, a verification request concerning a transaction, and means for causing transmission of a verification accept message in response to the processing indicating the transaction is acceptable, before a new block is established in the block chain.

[0018] According to an eighth aspect of the present invention, there is provided an apparatus comprising means for receiving a new transaction in a block chain based resource management system, means for causing transmission, to a verification node, of a verification request concerning the transaction, and means for transmitting the transaction to a network responsive to a verification accept message from the verification node, before a new block is established in the block chain.

[0019] According to a ninth aspect of the present invention, there is provided an apparatus comprising means for compiling a set of transactions in a block chain based resource management system that have taken place after the most recent block was established, means for establishing a new block in the block chain, and wherein in establishing the new block, for transactions associated with verification accept messages and lacking sufficient resources, the means for establishing are configured to cause transferring of the lacking resources from verification nodes having sent the verification accept messages.

[0020] According to a tenth aspect of the present invention, there is provided a non-transitory computer readable medium having stored thereon a set of computer readable instructions that, when executed by at least one processor, cause an apparatus to at least store a block chain segment of a block chain based resource management system, process, based at least partly on the block chain segment, a verification request concerning a transaction, and cause transmission of a verification accept message in response to the processing indicating the transaction is acceptable, before a new block is established in the block chain.

[0021] According to an eleventh aspect of the present invention, there is provided a non-transitory computer readable medium having stored thereon a set of computer readable instructions that, when executed by at least one processor, cause an apparatus to at least receive a new transaction in a block chain based resource management system, cause transmission, to a verification node, of a verification request concerning the transaction, and transmit the transaction to a network responsive to a verification accept message from the verification node, before a new block is established in the block chain.

[0022] According to a twelfth aspect of the present invention, there is provided a non-transitory computer readable medium having stored thereon a set of computer readable instructions that, when executed by at least one processor, cause an apparatus to at least compile a set of transactions in a block chain based resource management system that have taken place after the most recent block was established, establish a new block in the block chain, and wherein in establishing the new block, for transactions associated with verification accept messages and lacking sufficient resources, cause transferring of the lacking resources from verification nodes having sent the verification accept messages.

[0023] According to a thirteenth aspect of the present invention, there is provided a computer program configured to cause a method in accordance with at least one of the fourth, fifth or sixth aspects to be performed.

BRIEF DESCRIPTION OF THE DRAWINGS

[0024] FIGURE 1 illustrates an example system in accordance with at least some embodiments of the present invention;

[0025] FIGURE 2 illustrates an example process in accordance with at least some embodiments of the present invention;

[0026] FIGURE 3 illustrates an example apparatus capable of supporting at least some embodiments of the present invention;

[0027] FIGURE 4 illustrates an example process in accordance with at least some embodiments of the present invention;

[0028] FIGURE 5 is a first flow graph of a method in accordance with at least some embodiments of the present invention;

[0029] FIGURE 6 is a second flow graph of a method in accordance with at least some embodiments of the present invention, and

[0030] FIGURE 7 is a third flow graph of a method in accordance with at least some embodiments of the present invention.

EMBODIMENTS

[0031] In a block chain based resource management system, transaction delay may be reduced, and/or the resource double spending problem be alleviated, by verifying a transaction before a new block is established in the resource management system. The verifying may take place in a verification node comprised in the resource management system. The verification node may assume some risk from the verification procedure in case it chooses to verify a specific transaction. Block chain based resource management systems compatible with the present invention may manage various kinds resources, including, for example, file storage capacity, real-time ridesharing, smart contracts and digital cryptocurrency.

[0032] FIGURE 1 illustrates an example system in accordance with at least some embodiments of the present invention. A block chain based resource management system, referred to herein for the sake of brevity as "the system", is represented by nodes 101, 102, 103, 104, 105 and 110. These 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.

[0033] Nodes 101, 102, 103, 104, 105 and/or 110 maintain the block chain. This means that each node stores a segment of the block chain, wherein the segment may comprise the entire block chain or a part of the block chain. The segments in various nodes need not be of the same length. The block chain is an ordered sequence of blocks. When a new block is established, it is added to the block chain as a most recent established block.

The block chain may be a replicated, distributed database of transactions concerning the resources that are managed by the system. A block comprises a time-stamped batch of transactions. A block may further comprise a hash of a prior block, which immediately precedes the block in the block chain, linking thus the blocks together. A block may further comprise a proof-of-work, which will be described in more detail hereinbelow.

[0034] When the system is used, transactions are performed involving the resources that are managed by the system. Transactions performed since establishment of the most recent established block are included in the next block, that is, the next block in the sequence of blocks.

[0035] A transaction may comprise a transfer of resources to a recipient account. A transaction may comprise a data structure or message, which comprises an identifier and/or quantity of the resource to be transferred, an identifier of a recipient account and a cryptographic signature of the sender of the resource. Depending on the system, a sender account may also be identified in the transaction. Thus, the cryptographic signature, which is created using the private key of the sender, guards against theft of the resource, since only the sender is in possession of the private key.

[0036] To establish the next block, the transactions are broadcast into the network. Broadcasting here refers to a dissemination method suitable for the context, which will cause the transactions to be communicated to the nodes of the system in general. Reaching each and every node with each and every transaction is not strictly necessary. In case a transaction is verified, it may be broadcast into the network with verification information. Verification information may comprise an identity of a verification node that verified the transaction. A node establishing the next block may be known as a miner node. A miner node may compile a set of transactions, which it receives from the broadcasts, for the next block, and search for a proof-of-work code that covers all the transactions in the set of transactions for the next block. For example, the proof-of-work code may be a numerical value, with which the contents of the next block, that is, the set of transactions, hashes to a value that is less than a threshold. More generally, there may be a target area of an output space of a hash function, wherein the target space need not be in the low end of the target space. The smaller the target area is, the more difficult it is to discover the proof-of-work. Once a miner discovers the proof-of-work, it can publish the block, which other nodes of the system will then add to the block chain as the new most recent established block.

[0037] In case the miner node discovers a proof-or-work based on an incomplete set of transactions, for example if some transactions didn't reach the miner node, other nodes in the network will not accept the block into the block chain, and it will be excluded from a consensus version of the block chain in the system.

[0038] Since an output of a hash function is a pseudorandom function of the input, the set of transactions, hashed by itself, produces a hash value that is essentially randomly placed in the output space of the hash function. Note, that the set of transactions may be completely or representatively present as input to the hash function. Modifying the input with a candidate proof-of-work code, which may be known as a nonce, will produce a new hash value, which again is essentially randomly placed in the output space of the hash function. The modification may be as slight as a single bit. Therefore, searching for the correct proof-of-work code, which satisfies a pre-agreed criterion concerning its location in the output space of the hash function, requires repeatedly deriving a hash value with a different candidate proof-of-work code modifying the input to the hash function. Once a proof-of-work code that, with the transactions, produces a hash value in the target area of the output space of the hash function is found, the block is ready. A ready block may be distributed to the system to establish it therein in the block chain.

[0039] Once a new block is established, the block chain becomes longer. A transaction is considered the more reliable, the larger the number of blocks established since the block where the transaction is comprised. This is so, since a transactions are hashed into the chain of blocks, and discrepancies in the block chain are resolved as the block chain gets longer. In detail, maliciously modifying a transaction in a block far down the chain would involve re-doing the work of finding proofs-of-work for all subsequent blocks, since the input to the hash function for the block comprising the transaction would be changed, causing the resulting hash value, with the proof-of-work in that block, to no longer be disposed in the desired area in the output space of the hash function.

[0040] Where the time between block establishments is long, say, 10 or 15 minutes, an uncertainty as to a validity of a transaction may arise until the next block is established. In principle, an owner might send the same resource to two recipients in two transactions. This would be discovered in connection with establishing the next block, since there would be two competing owners of the resource, but this would not necessarily be immediately recognized.

[0041] A verification node, comprised in the system, may overcome problems related to the delay between consecutive block establishments. In terms of FIGURE 1, considering for the sake of illustration a cryptocurrency system, a merchant 120 may sell an item to customer 130. In connection with releasing the item to customer 130, merchant 120 may request payment in the cryptocurrency. This request is illustrated as message 123 in FIGURE 1. Responsively, customer 130 compiles a transaction and provides it to merchant 120. This is illustrated as message 132 in FIGURE 1.

[0042] To verify the transaction, merchant 120 may provide the transaction to verification node 110, in message 121. Verification node 110, responsive to verifying the transaction, may provide a verification acceptance message 112 to merchant 120 as a response to message 121. Message 121 may be seen as a verification request of the transaction. A verification request may comprise the transaction, or a link to the transaction. Responsive to verification acceptance message 112, merchant 120 may release the item to customer 130. Verification acceptance message 112 may comprise a cryptographic signature of verification node 110. An advantage is therefore gained, for example, where customer 130 seeks to buy access rights to digital content, since the sale may be reliably completed without waiting for the next block to be established. Verification acceptance message 112 may be transmitted to the node that sent the verification request message 121, in this case merchant 120. Verification acceptance message 112 may be transmitted also to at least one further verification node.

[0043] Verification node 110 may store a segment of the block chain, like other nodes in the system. Processing verification request 121 may comprise checking, based on the block chain segment, that customer 130 is the present owner of the resources the transaction involves, that is, customer 130 is seeking to use his own resources. In case customer 130 is not the current owner of the resources, verification node 110 may decide to either simply not send the verification accept message 112, or to send instead a verification refused message. In case the verification based on the block chain segment fails, it may be beneficial to wait for establishment of the next block in the block chain, to resolve the conflict. In this sense, transmitting a verification refuse message may be unnecessary.

[0044] Processing the verification request may comprise checking the cryptographic signature in the transaction has been produced with the correct private key. Where the

cryptographic signature fails verification, it may be unnecessary to even check if customer 130 overall has sufficient resources for the transaction.

[0045] Processing may comprise checking that verification node 110 is not aware of any previous transaction, by the owner of the resource, concerning the resource, after establishment of the most recent block. This mitigates the double spending problem.

[0046] Processing the verification request may comprise checking, whether resources owned by a verification node would, in the transaction, be transferred to another owner. Verification node 110 may be configured to reject, or not verify, such transactions. Likewise, processing the verification request may comprise checking whether verification node 110 has a quantity of resources sufficient to cover the transaction, in case it turns out to lack resources in connection with establishing the next block. Verification node 110 may be configured to not verify transactions that involve transferring mode resources than verification node has at its disposal.

[0047] Processing the verification request may comprise collaborating with other verification nodes. For example, where verification node 110 determines a block in the block chain that verification node 110 doesn't have would be needed, verification node 110 may request older blocks from other verification nodes. Alternatively, collaborating may comprise verification node 110 transmitting the verification request to at least one further verification node. In some embodiments, verification node 110 distributes the verification request to a set of verification nodes, and receives responses from the set of verification nodes. Verification node 110 may then transmit the verification accept message merchant 120 if, and only if, none of the responses from the set of verification nodes is a rejection of the transaction. Using a set of verification nodes may be useful in guarding against the double spending problem, since other verification nodes may know of a prior transaction involving the same resource as the transaction, which the resource owner has made in another part of the system, after the most recent block establishment.

[0048] When the time comes to establish the next block in the block chain, a node establishing the block may compile, as described above, a set of transactions that have taken place since the most recent established block. The next block will comprise this set of transactions. In connection with establishing the next block, the node may identify which transactions lack resources, that is, which transactions involve resources that the resource sender does not control. This may be the case, for example, in case the sender has

compiled a fraudulent transaction involving transferring resources the sender doesn't own to a recipient. From among the transactions lacking resources, the node may identify those that have been verified by a verification node, that is, those transactions concerning which a verification node has transmitted a verification acceptance message. Transactions lacking resources that have not been verified may be discarded when compiling the set of transactions for the next block, for example.

[0049] For each verified transaction lacking resources, the node may cause transferring of resources owned by the verification node that verified the transaction, to make up for the missing resources. In other words, the verification node may be made to make up for a loss that a merchant would otherwise have incurred from the transaction. The node may cause the transferring, for example, by compiling a new transaction that transfers resources of the verification node to the recipient of the original verified transaction that lacks resources. The new transaction may be included in the block being prepared for establishment, as other nodes in the system are also enabled to generate the new transaction, wherefore the new transaction, in some embodiments, doesn't need to be propagated in the system. This reduces the delay in handling transactions lacking resources.

[0050] Verification nodes may be configured to charge merchants a fee, in terms of resources, for verifying transactions, to thereby obtain resources for making up for erroneously verified transactions that lack resources. The fee may be 0.1%, 1% or 2% of the amount of resources involved in the transaction to be verified, for example. In this sense, the verification function may be seen as a form of insurance in addition to speeding-up of the transaction clearing.

[0051] In some embodiments, the system maintains a list of nodes authorized to issue verification accept messages, and thereby verify transactions. Further, in some embodiments, verification nodes maintain a block chain distinct from the one maintained in the system nodes. The block chain in verification nodes may then be based, instead of a proof-of-work principle, on a proof-of-stake principle. In a proof-of-stake block chain, rather than demonstrating that computational work has been done, a node needs to demonstrate ownership of a certain amount of resources. This could raise an entry barrier to commit fraud, since an imposter would need to control at least one verification node, 51% of computational power in the proof-of-work nodes and a 51% stake of resources in

the system. In a proof-of-stake system, a block chain maintained by verification nodes may be a separate, secondary chain based on proof-of-stake. To compromise the overall system, an attacker would need to compromise both the main block chain based on proof-of-work and the secondary block chain based on proof-of-stake, since the same transactions would be recorded in both block chains. In practice, a proof-of-stake block chain may provide an advantage in that less energy is spent than in a proof-of-work block chain, since the proof-of-work method may require a large input of numerical computer calculation resources, which consume energy.

[0052] FIGURE 2 illustrates an example process in accordance with at least some embodiments of the present invention. The process may take place in a verification node, for example. In phase 210, the verification node, being in receipt of a verification request, may check whether the transaction the verification request concerns is valid according to a system consensus. This may comprise checking the cryptographic signature is correct, for example, and/or checking the transaction does not seek to transfer resources of a verification node.

[0053] In phase 220, the verification node may check the sender is in possession of the resources the transaction seeks to transfer to a new owner, or recipient. In case this is not the case, that is, if the transaction lacks resources, processing may proceed to phase 260, where a decision is taken to not verify the transaction. Where the verification is declined, a message to that effect may be transmitted to the merchant, however this is not a mandatory step and is absent in some embodiments.

[0054] Where phase 230 indicates the sender is indeed in possession of the resources the transaction involves, the verification node may send a verification acceptance message to other verification nodes, phase 240, and to the merchant, phase 250.

[0055] In general, when a transaction that is verified is broadcast to the system, the broadcasting may comprise verification information, which may identify the verification node that verified the transaction. Therefore, when the next block will be established, the nodes establishing the next block may easily determine that the transaction is of the verified type, and which verification node verified it. This broadcasting may be initiated by verification node 110 or merchant 120, for example.

[0056] FIGURE 3 illustrates an example apparatus capable of supporting at least some embodiments of the present invention. Illustrated is device 300, which may comprise, for example, merchant 120, verification node 110, client device 130, or a system node such as node 101, 102, 103, 104 and/or 105, in applicable parts, of FIGURE 1. Comprised in device 300 is processor 310, 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. Processor 310 may comprise more than one processor. A processing core may comprise, for example, a Cortex-A8 processing core manufactured by ARM Holdings or a Steamroller processing core produced by Advanced Micro Devices Corporation. Processor 310 may comprise at least one Qualcomm Snapdragon and/or Intel Atom processor. Processor 310 may comprise at least one application-specific integrated circuit, ASIC. Processor 310 may comprise at least one field-programmable gate array, FPGA. Processor 310 may be means for performing method steps in device 300. Processor 310 may be configured, at least in part by computer instructions, to perform actions.

[0057] Device 300 may comprise memory 320. Memory 320 may comprise random-access memory and/or permanent memory. Memory 320 may comprise at least one RAM chip. Memory 320 may comprise solid-state, magnetic, optical and/or holographic memory, for example. Memory 320 may be at least in part accessible to processor 310. Memory 320 may be at least in part comprised in processor 310. Memory 320 may be means for storing information. Memory 320 may comprise computer instructions that processor 310 is configured to execute. When computer instructions configured to cause processor 310 to perform certain actions are stored in memory 320, and device 300 overall is configured to run under the direction of processor 310 using computer instructions from memory 320, processor 310 and/or its at least one processing core may be considered to be configured to perform said certain actions. Memory 320 may be at least in part comprised in processor 310. Memory 320 may be at least in part external to device 300 but accessible to device 300.

[0058] Device 300 may comprise a transmitter 330. Device 300 may comprise a receiver 340. Transmitter 330 and receiver 340 may be configured to transmit and receive, respectively, information in accordance with at least one cellular or non-cellular standard. Transmitter 330 may comprise more than one transmitter. Receiver 340 may comprise more than one receiver. Transmitter 330 and/or receiver 340 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, WiMAX, standards, for example.

[0059] Device 300 may comprise a near-field communication, NFC, transceiver 350. NFC transceiver 350 may support at least one NFC technology, such as NFC, Bluetooth, Wibree or similar technologies.

[0060] Device 300 may comprise user interface, UI, 360. UI 360 may comprise at least one of a display, a keyboard, a touchscreen, a vibrator arranged to signal to a user by causing device 300 to vibrate, a speaker and a microphone. A user may be able to operate device 300 via UI 360, for example to initiate transactions.

[0061] Device 300 may comprise or be arranged to accept a user identity module 370. User identity module 370 may comprise, for example, a subscriber identity module, SIM, card installable in device 300. A user identity module 370 may comprise information identifying a subscription of a user of device 300. A user identity module 370 may comprise cryptographic information usable to verify the identity of a user of device 300 and/or to facilitate encryption of communicated information and billing of the user of device 300 for communication effected via device 300.

[0062] Processor 310 may be furnished with a transmitter arranged to output information from processor 310, via electrical leads internal to device 300, to other devices comprised in device 300. Such a transmitter may comprise a serial bus transmitter arranged to, for example, output information via at least one electrical lead to memory 320 for storage therein. Alternatively to a serial bus, the transmitter may comprise a parallel bus transmitter. Likewise processor 310 may comprise a receiver arranged to receive information in processor 310, via electrical leads internal to device 300, from other devices comprised in device 300. Such a receiver may comprise a serial bus receiver arranged to, for example, receive information via at least one electrical lead from receiver 340 for processing in processor 310. Alternatively to a serial bus, the receiver may comprise a parallel bus receiver.

[0063] Device 300 may comprise further devices not illustrated in FIGURE 3. For example, where device 300 comprises a smartphone, it may comprise at least one digital

camera. Some devices 300 may comprise a back-facing camera and a front-facing camera, wherein the back-facing camera may be intended for digital photography and the front-facing camera for video telephony. Device 300 may comprise a fingerprint sensor, or other biometric sensor, arranged to authenticate, at least in part, a user of device 300. In some embodiments, device 300 lacks at least one device described above. For example, some devices 300 may lack a NFC transceiver 350 and/or user identity module 370.

[0064] Processor 310, memory 320, transmitter 330, receiver 340, NFC transceiver 350, UI 360 and/or user identity module 370 may be interconnected by electrical leads internal to device 300 in a multitude of different ways. For example, each of the aforementioned devices may be separately connected to a master bus internal to device 300, to allow for the devices to exchange information. However, as the skilled person will appreciate, this is only one example and depending on 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.

[0065] FIGURE 4 illustrates an example process in accordance with at least some embodiments of the present invention. The process of FIGURE 4 relates to establishing a next block in the block chain.

[0066] Initially, in phase 410, a node compiles an initial set of transactions that have occurred since establishment of the most recent established block. In optional phase 420, transactions that seek to transfer resources of verification nodes are discarded. In phase 430, transactions in the set of transactions are ordered according to times, when they appeared in the system. For example, older transactions are arranged before newer ones.

[0067] Phase 440 proceeds, for each transaction not seeking to transfer resources of a verification node, to phase 450. In phase 450, it is checked, whether the sender of the transaction controls the resource the transaction seeks to transfer. In case this is the case, the transaction is left in the set and processing advances to phase 460, and if not, processing advances to phase 4120.

[0068] In phase 460, the transaction is applied to the new block, and processing proceeds to phase 470, where it is checked, whether there are further transactions. If there are further transactions, processing advances back to phase 440, and if not, processing advances to phase 480. In phase 480, transactions that do transfer resources to, or from,

verification nodes are processed, such that in phase 490 these transactions are applied to the new block. Once also these transactions are applied, the block is ready for establishment. The proof-of-work is calculated in phase 4100, and once it is found, the new block is published in phase 4110. Phases 4110 and 4110 make the establishment of the new block effective in the system.

[0069] Returning then to the case where it is, in phase 450, determined the sender does not control the resource the transaction seeks to transfer. In this case, processing advances, as described above, to phase 4120. In phase 4120, it is in turn checked, whether the transaction was verified, that is, whether a verification node transmitted a verification acceptance message concerning the transaction. If this was not done, that is, if the transaction was not verified, processing advances to phase 4130, where the transaction is discarded, and therefrom again to phase 440. Discarding the transaction in this context means the transaction is not included in the new block.

[0070] If, on the other hand, it is in phase 4120 determined the transaction was in fact verified, processing advances to phase 4140, where resources corresponding to those lacking are caused to be transferred from a verification node that verified the transaction, to the recipient of the verified transaction that lacks resources. For example a new transaction may be entered into the new block, which transfers the lacking resources from the verification node to the recipient of the transaction. From phase 4140, processing advances back to phase 470. In this exceptional case, the new transaction may lack a cryptographic signature of the verification node for this specific new transaction, but a cryptographic signature of the verification node may be present in the verification accept message and/or the verification information broadcast with the transaction. The system may be configured to accept such a cryptographic signature as an acceptance of the verification node to transfer its resources in a situation where the verified transaction is found to lack resources.

[0071] In general, that is, not only relating to FIGURE 4, where a group of verification nodes together verified the transaction lacking resources, the group may share the burden of making up for the lacking resources.

[0072] FIGURE 5 is a first flow graph of a method in accordance with at least some embodiments of the present invention. The phases of the illustrated method may be

performed in verification node 110, or in a control device configured to control the functioning thereof, when implanted therein.

[0073] Phase 510 comprises storing, in an apparatus, a block chain segment of a block chain based resource management system. Phase 520 comprises processing, based at least partly on the block chain segment, a verification request concerning a transaction. Phase 530 comprises causing transmission of a verification accept message in response to the processing indicating the transaction is acceptable, before a new block is established in the block chain.

[0074] FIGURE 6 is a second flow graph of a method in accordance with at least some embodiments of the present invention. The phases of the illustrated method may be performed in merchant 120, or in a control device configured to control the functioning thereof, when implanted therein.

[0075] Phase 610 comprises receiving a new transaction in a block chain based resource management system. Phase 620 comprises causing transmission, to a verification node, of a verification request concerning the transaction. Phase 630 comprises transmitting the transaction to a network responsive to a verification accept message from the verification node, before a new block is established in the block chain.

[0076] FIGURE 7 is a third flow graph of a method in accordance with at least some embodiments of the present invention. The phases of the illustrated method may be performed in a miner node, or in a control device configured to control the functioning thereof, when implanted therein.

[0077] Phase 710 comprises compiling a set of transactions in a block chain based resource management system that have taken place after the most recent block was established. Phase 720 comprises establishing a new block in the block chain. Phase 730 comprises, in establishing the new block, for transactions associated with verification accept messages and lacking sufficient resources, causing transferring of the lacking resources from verification nodes having sent the verification accept messages. The new block is the next block in the block chain.

[0078] 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

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.

[0079] Reference 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 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. Where reference is made to a numerical value using a term such as, for example, about or substantially, the exact numerical value is also disclosed.

[0080] As used herein, a plurality of items, structural elements, compositional elements, and/or materials may be presented in a common list for convenience. However, these lists should be construed as though each member of the list is individually identified as a separate and unique member. Thus, no individual member of such list should be construed as a de facto equivalent of any other member of the same list solely based on their presentation in a common group without indications to the contrary. In addition, various embodiments and example of the present invention may be referred to herein along with alternatives for the various components thereof. It is understood that 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.

[0081] Furthermore, the described features, structures, or characteristics may be combined in any suitable manner in one or more embodiments. In the preceding 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 described in detail to avoid obscuring aspects of the invention.

[0082] 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 principles and concepts of the invention. Accordingly, it is not intended that the invention

be limited, except as by the claims set forth below.

[0083] 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 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

[0084] At least some embodiments of the present invention find industrial application in verifying cryptographic transactions.

ACRONYMS LIST

IP internet protocol

REFERENCE SIGNS LIST

110	Verification node
120	Merchant
130	Customer
101, 102, 103, 104, 105	System nodes, at least some of which may also be miner nodes
210 – 250	Phases of the method of FIGURE 2
300-370	Structure of the apparatus of FIGURE 3
410-4140	Phases of the method of FIGURE 4
510-530	Phases of the method of FIGURE 5
610-630	Phases of the method of FIGURE 6
710-730	Phases of the method of FIGURE 7

CLAIMS:

1. An apparatus comprising:
   - memory configured to store a block chain segment of a block chain based resource management system;
   - at least one processing core configured to process, based at least partly on the block chain segment, a verification request concerning a transaction, and to cause transmission of a verification accept message in response to the processing indicating the transaction is acceptable, before a new block is established in the block chain.

2. The apparatus according to claim 1, wherein the at least one processing core is configured to process the verification request at least partly by determining, whether a cryptographic signature comprised in the verification request is associated with sufficient resources to perform the transaction.

3. The apparatus according to any of claims 1 - 2, wherein the at least one processing core is configured to process the verification request at least partly by determining, whether resources of a verification node would be transferred in the transaction.

4. The apparatus according to any of claims 1 – 3, wherein the apparatus comprises a verification node, and the at least one processing core is configured to process the verification request at least partly in collaboration with other verification nodes.

5. The apparatus according to claim 4, wherein the collaboration comprises transmitting the verification request to the other verification nodes.

6. The apparatus according to claim 4, wherein the collaboration comprises requesting further block chain segments from the other verification nodes.

7. The apparatus according to any of claims 1 – 6, wherein the verification accept message comprises a cryptographic signature of the apparatus.

8. The apparatus according to claim 7, wherein the apparatus is configured to transmit the verification accept message to the node that sent the verification request message to the apparatus.

9. The apparatus according to claim 7 or 8, wherein the apparatus is configured to transmit the verification accept message to at least one further verification node.

10. 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 configured to, with the at least one processing core, cause the apparatus at least to:

- receive a new transaction in a block chain based resource management system;
- cause transmission, to a verification node, of a verification request concerning the transaction, and
- transmit the transaction to a network responsive to a verification accept message from the verification node, before a new block is established in the block chain.

11. 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 configured to, with the at least one processing core, cause the apparatus at least to:

- compile a set of transactions in a block chain based resource management system that have taken place after the most recent block was established;
- establish a new block in the block chain, and
- in establishing the new block, for transactions associated with verification accept messages and lacking sufficient resources, cause transferring of the lacking resources from verification nodes having sent the verification accept messages.

12. The apparatus according to claim 11, wherein the at least one memory and the computer program code are configured to, with the at least one processing core, cause the transferring of the lacking resources by including, for each transaction associated with a verification accept message and lacking sufficient resources, in the new block, a transaction that transfers resources from the verification node that sent the associated verification message to a recipient of the transaction lacking sufficient resources.

13. A method comprising:

- storing, in an apparatus, a block chain segment of a block chain based resource management system;
- processing, based at least partly on the block chain segment, a verification request concerning a transaction, and
- causing transmission of a verification accept message in response to the processing indicating the transaction is acceptable, before a new block is established in the block chain.

14. The method according to claim 13, wherein the processing of the verification request comprises determining, whether a cryptographic signature comprised in the verification request is associated with sufficient resources to perform the transaction.

15. The method according to any of claims 13 - 14, wherein the processing of the verification request comprises determining, whether resources of a verification node would be transferred in the transaction.

16. The method according to any of claims 13 – 15, wherein the apparatus comprises a verification node, and the processing of the verification request comprises collaborating with other verification nodes.

17. The method according to claim 16, wherein the collaborating comprises transmitting the verification request to the other verification nodes.

18. The method according to claim 16, wherein the collaborating comprises requesting further block chain segments from the other verification nodes.

19. The method according to any of claims 13 – 18, wherein the verification accept message comprises a cryptographic signature of the apparatus.

20. The method according to claim 19, wherein the verification accept message is transmitted to the node that sent the verification request message to the apparatus.

21. The method according to claim 19 or 20, further comprising transmitting the verification accept message to at least one further verification node.

22. A method, comprising:

- receiving a new transaction in a block chain based resource management system;
- causing transmission, to a verification node, of a verification request concerning the transaction, and
- transmitting the transaction to a network responsive to a verification accept message from the verification node, before a new block is established in the block chain.

23. A method, comprising:

- compiling a set of transactions in a block chain based resource management system that have taken place after the most recent block was established;
- establishing a new block in the block chain, and
- in establishing the new block, for transactions associated with verification accept messages and lacking sufficient resources, causing transferring of the lacking resources from verification nodes having sent the verification accept messages.

24. The method according to claim 11, further comprising causing the transferring of the lacking resources by including, for each transaction associated with a verification accept message and lacking sufficient resources, in the new block, a transaction that transfers resources from the verification node that sent the associated verification message to a recipient of the transaction lacking sufficient resources.

25. An apparatus comprising:

- means for storing a block chain segment of a block chain based resource management system;
- means for processing, based at least partly on the block chain segment, a verification request concerning a transaction, and
- means for causing transmission of a verification accept message in response to the processing indicating the transaction is acceptable, before a new block is established in the block chain.

26. An apparatus comprising:

- means for receiving a new transaction in a block chain based resource management system;
- means for causing transmission, to a verification node, of a verification request concerning the transaction, and
- means for transmitting the transaction to a network responsive to a verification accept message from the verification node, before a new block is established in the block chain.

27. An apparatus comprising:

- means for compiling a set of transactions in a block chain based resource management system that have taken place after the most recent block was established;
- means for establishing a new block in the block chain, and
- wherein in establishing the new block, for transactions associated with verification accept messages and lacking sufficient resources, the means for establishing are configured to cause transferring of the lacking resources from verification nodes having sent the verification accept messages.

28. A non-transitory computer readable medium having stored thereon a set of computer readable instructions that, when executed by at least one processor, cause an apparatus to at least:

- store a block chain segment of a block chain based resource management system;
- process, based at least partly on the block chain segment, a verification request concerning a transaction, and
- cause transmission of a verification accept message in response to the processing indicating the transaction is acceptable, before a new block is established in the block chain.

29. A non-transitory computer readable medium having stored thereon a set of computer readable instructions that, when executed by at least one processor, cause an apparatus to at least:

- receive a new transaction in a block chain based resource management system;
- cause transmission, to a verification node, of a verification request concerning the transaction, and
- transmit the transaction to a network responsive to a verification accept message from the verification node, before a new block is established in the block chain.

30. A non-transitory computer readable medium having stored thereon a set of computer readable instructions that, when executed by at least one processor, cause an apparatus to at least:

- compile a set of transactions in a block chain based resource management system that have taken place after the most recent block was established;
- establish a new block in the block chain, and
- wherein in establishing the new block, for transactions associated with verification accept messages and lacking sufficient resources, cause transferring of the lacking resources from verification nodes having sent the verification accept messages.

31. A computer program configured to cause a method in accordance with at least one of claims 13 – 24 to be performed.

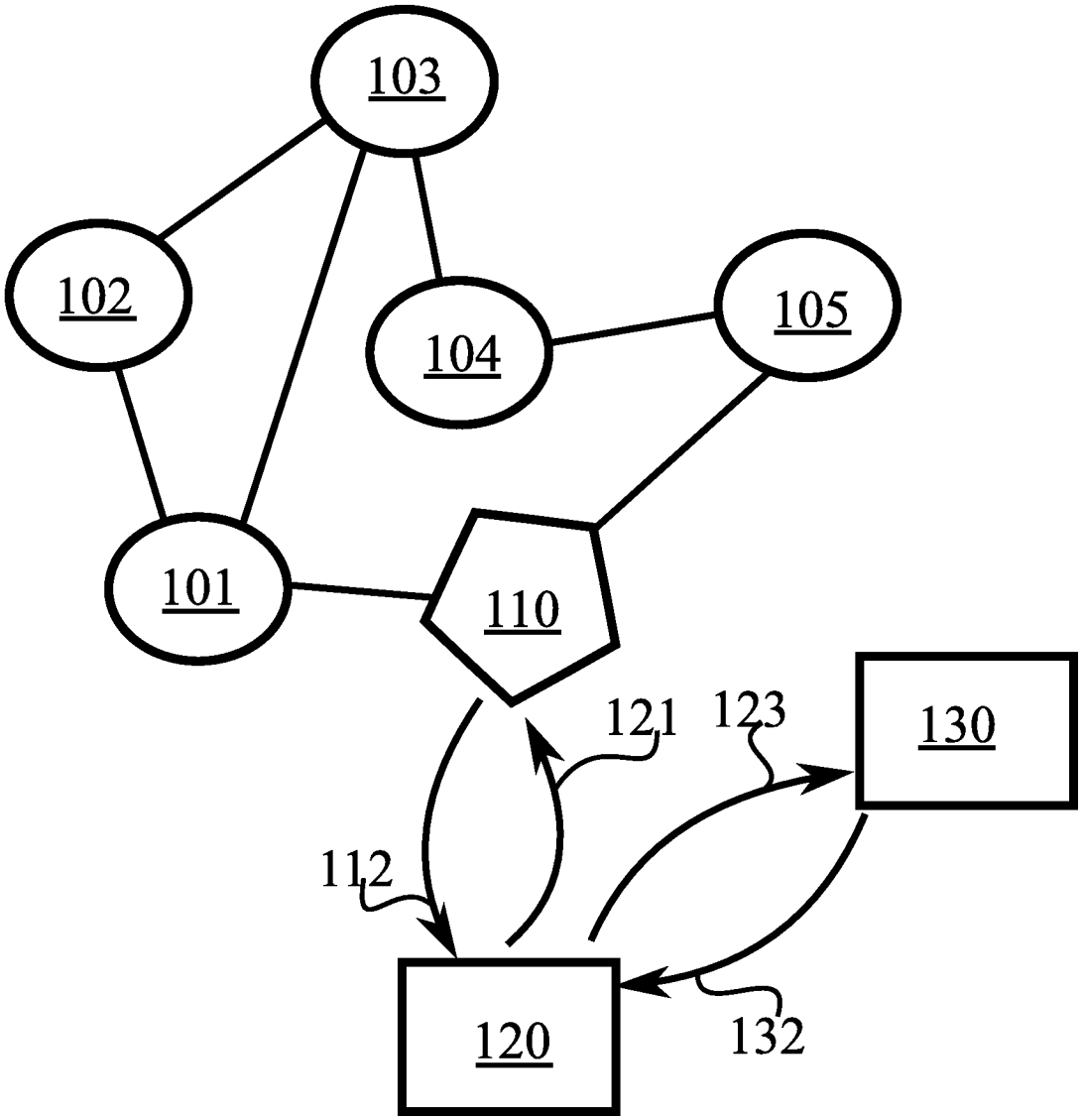

FIGURE 1

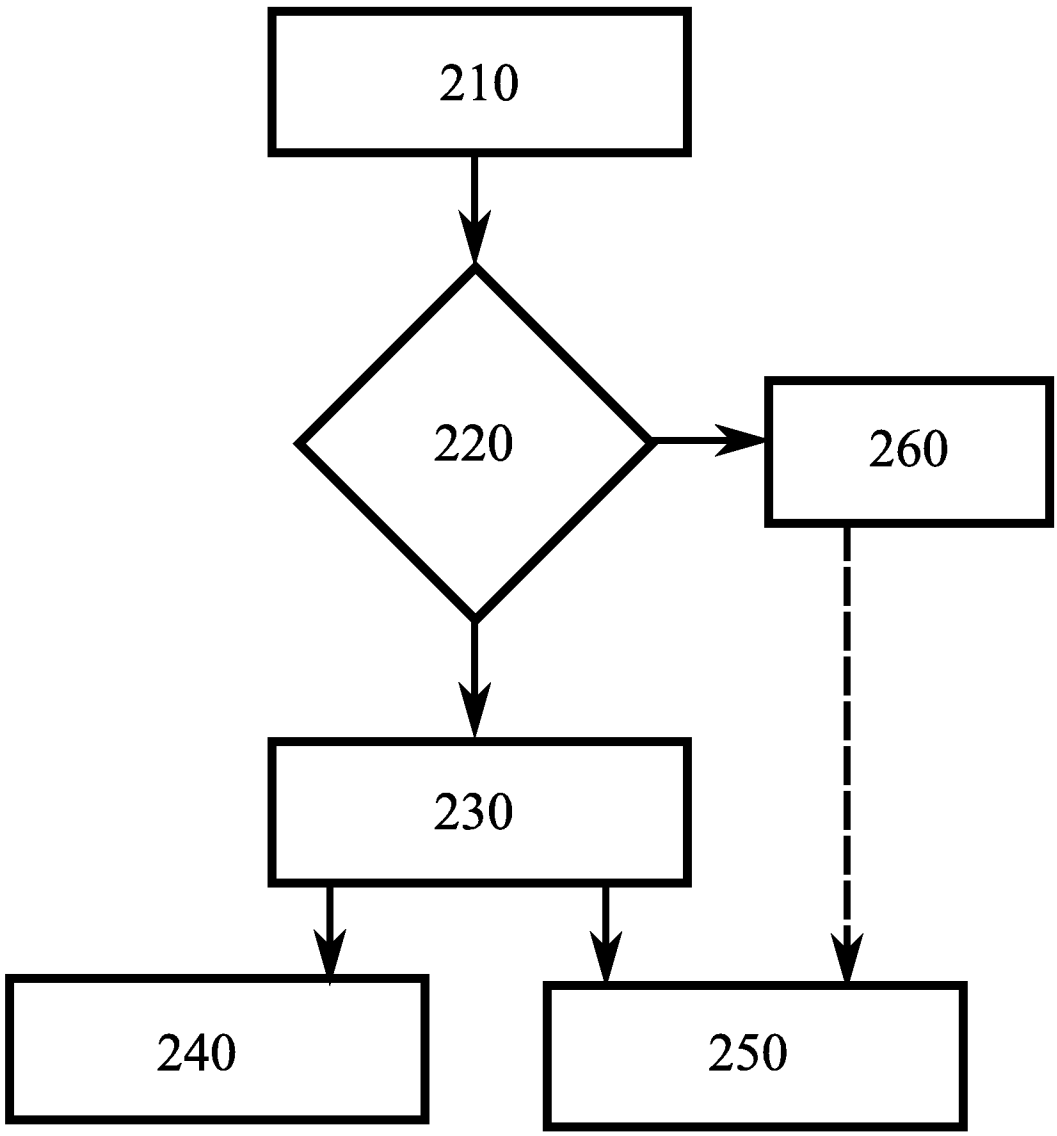

FIGURE 2

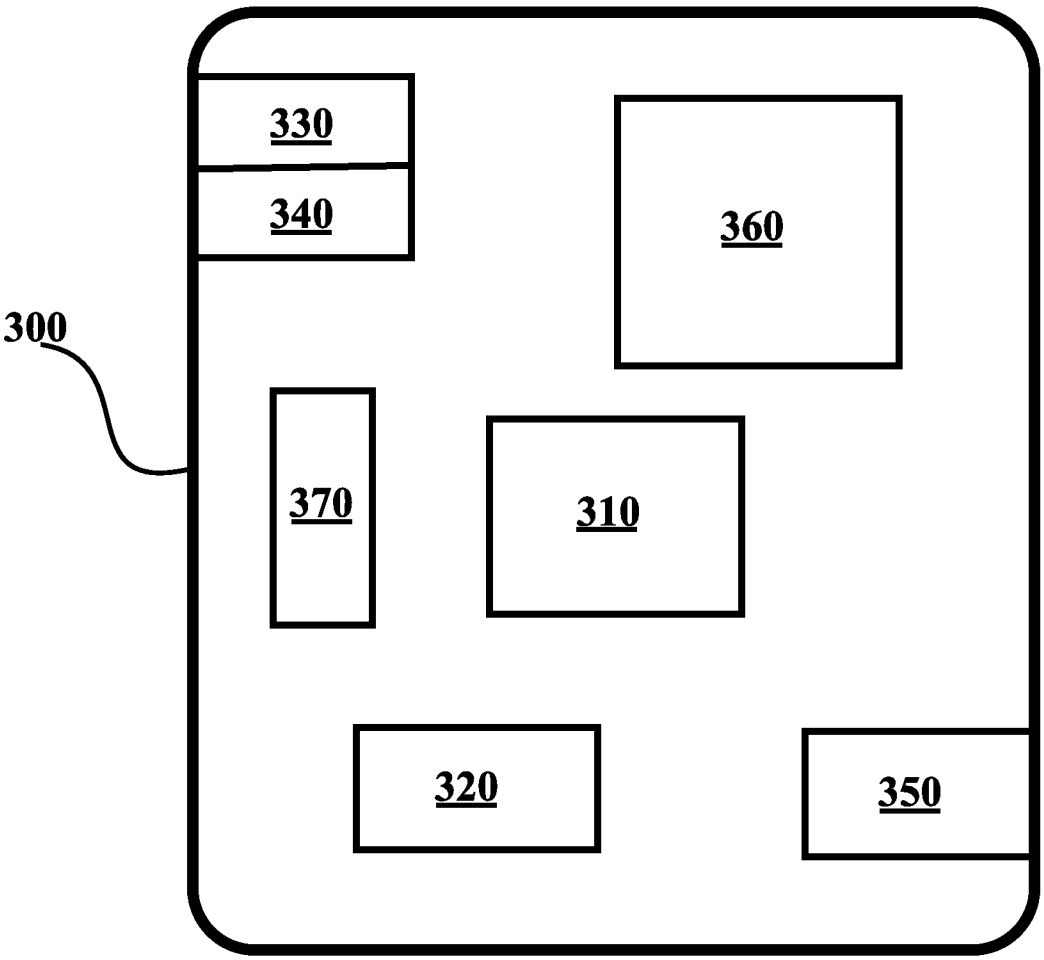

FIGURE 3

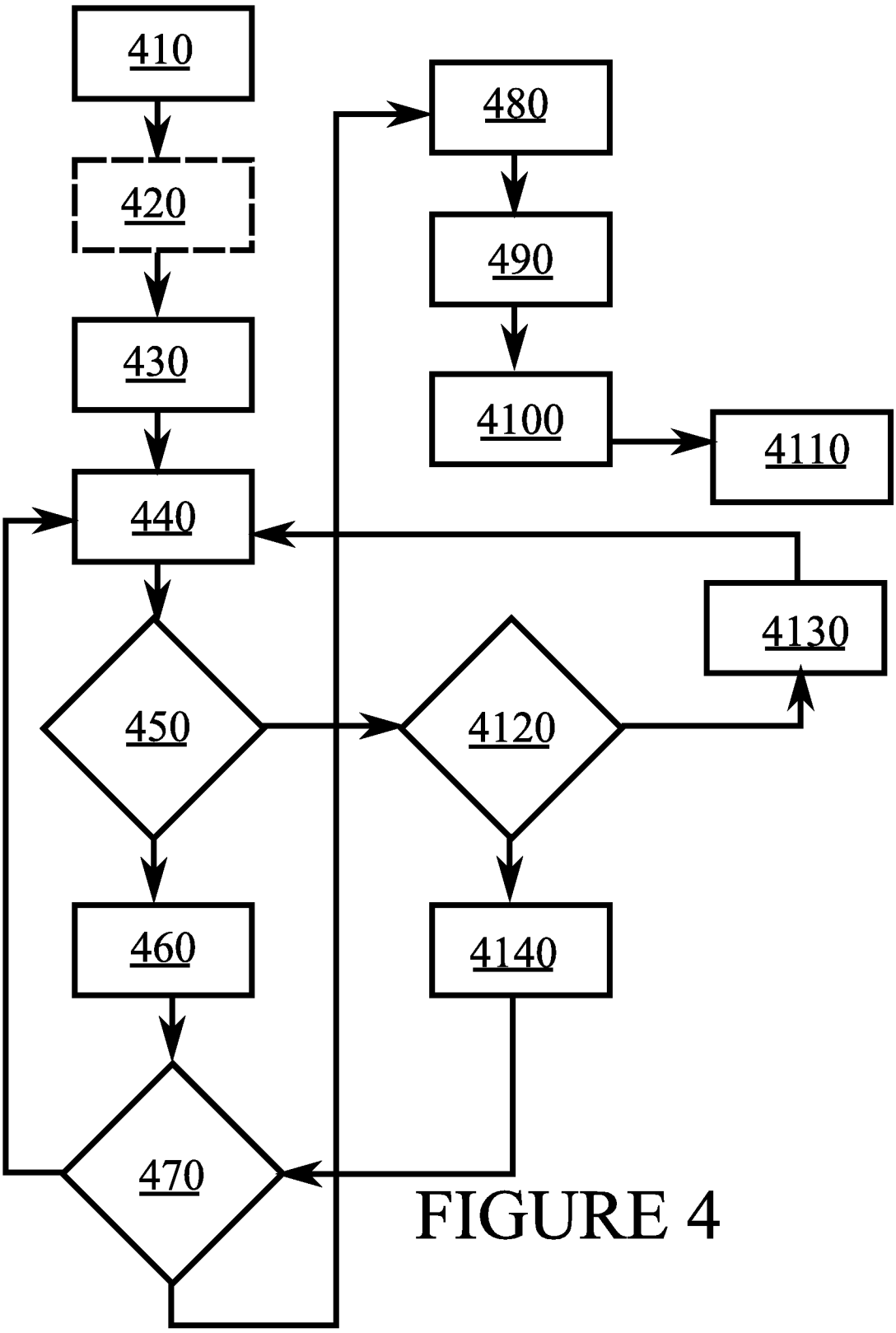

FIGURE 4

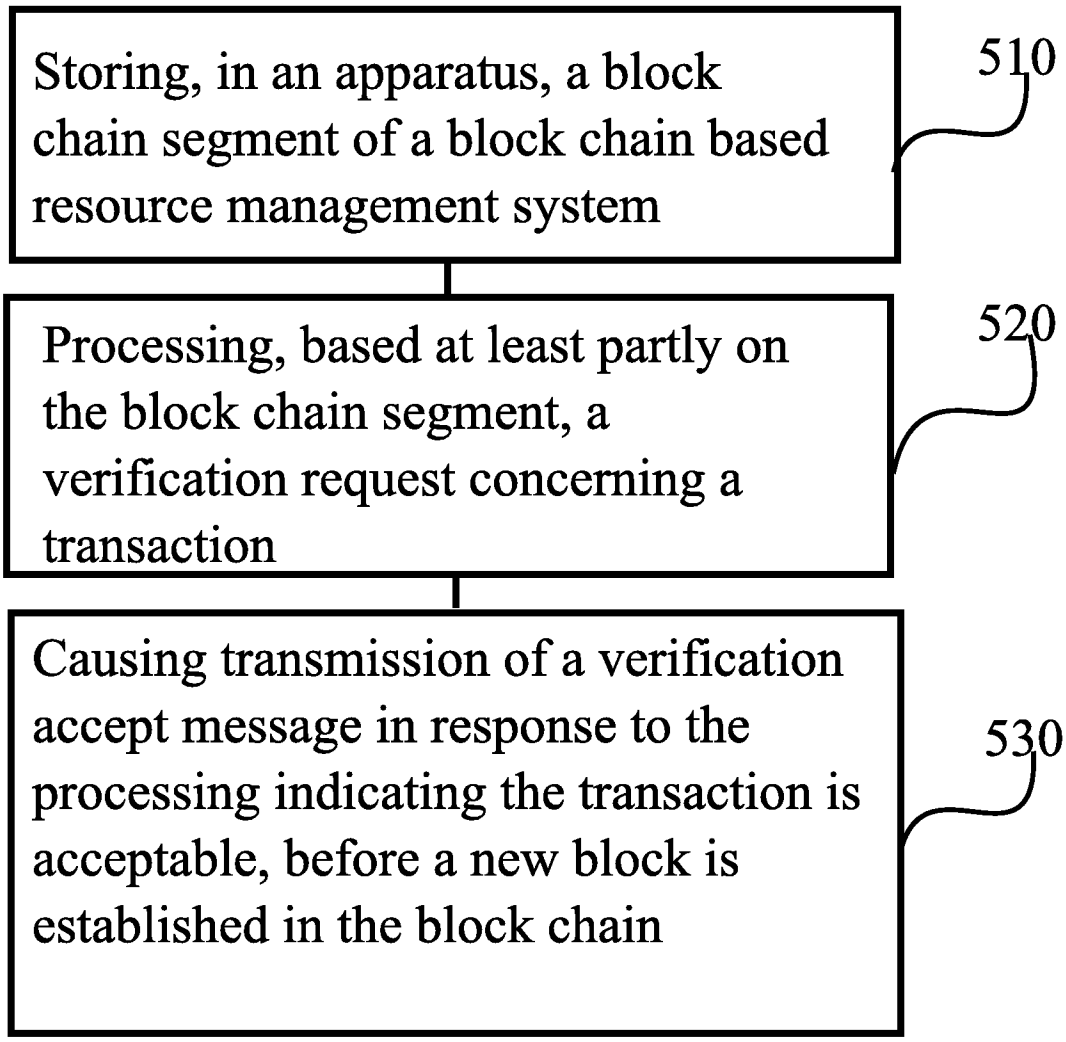
Storing, in an apparatus, a block chain segment of a block chain based resource management system
510
Processing, based at least partly on the block chain segment, a verification request concerning a transaction
520
Causing transmission of a verification accept message in response to the processing indicating the transaction is acceptable, before a new block is established in the block chain
530

FIGURE 5

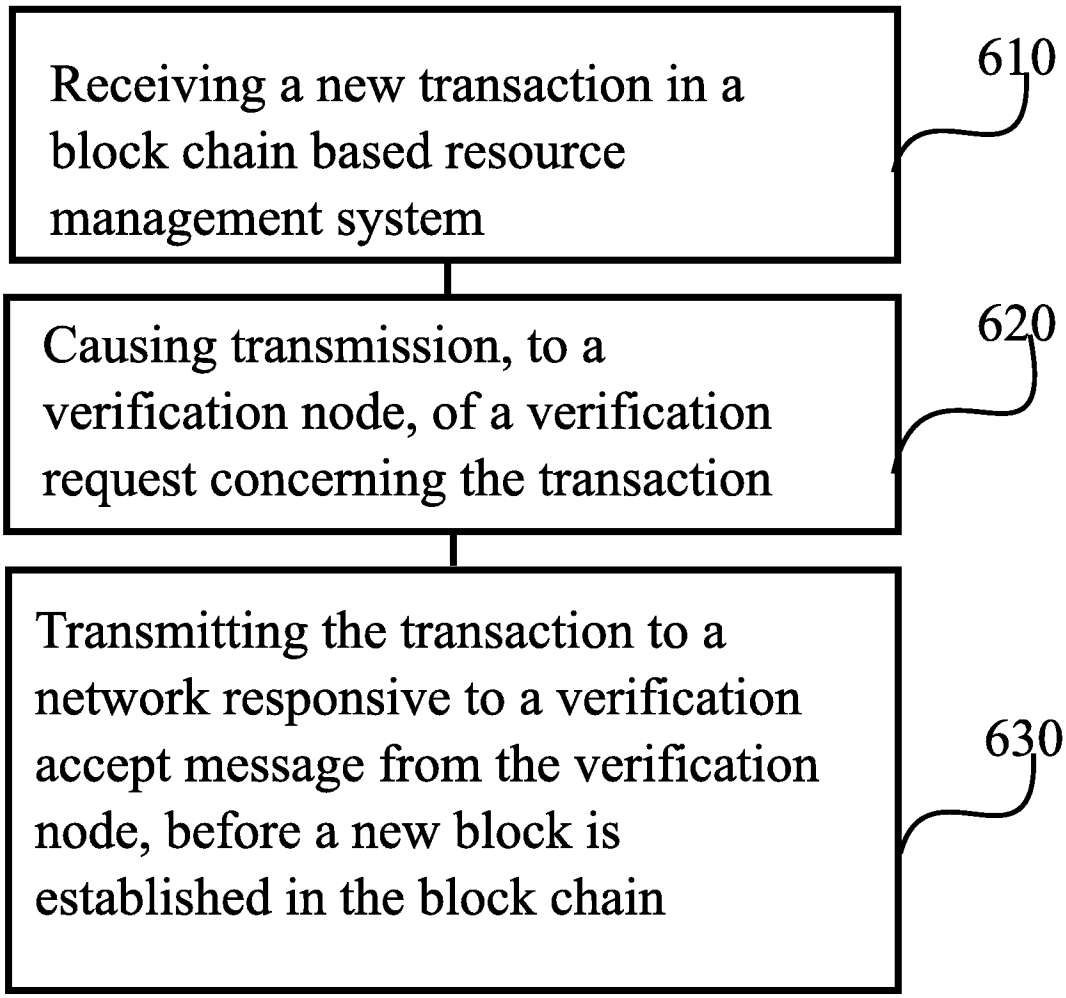
Receiving a new transaction in a block chain based resource management system
610
Causing transmission, to a verification node, of a verification request concerning the transaction
620
Transmitting the transaction to a network responsive to a verification accept message from the verification node, before a new block is established in the block chain
630

FIGURE 6

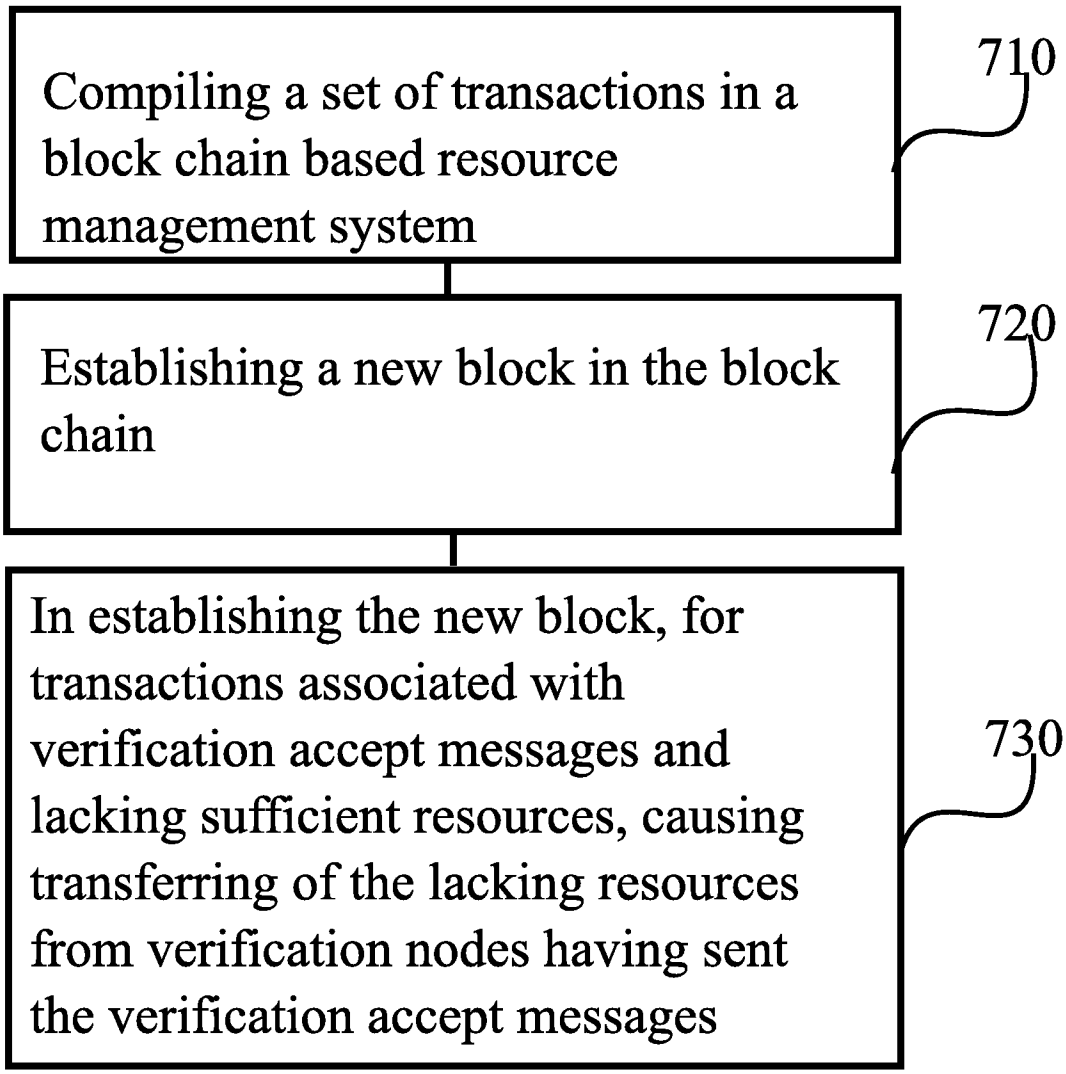
Compiling a set of transactions in a block chain based resource management system
710
Establishing a new block in the block chain
720
In establishing the new block, for transactions associated with verification accept messages and lacking sufficient resources, causing transferring of the lacking resources from verification nodes having sent the verification accept messages
730

FIGURE 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2016/050187

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: H04L, H04W, 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, XP3GPP, XPAIP, XPESP, XPETSI, XPI3E, XPIEE, XPIETF, XPIOP, XPIPCOM, XPJPEG, XPMISC, XPOAC, XPRD, XPTK, BIOSIS, COMPDX, INSPEC, MEDLINE, TDB, NPL, PRH-Internal, Internet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2015363782 A1 (RONCA JAMES G [US] et al.) 17 December 2015 (17.12.2015) abstract; Figs. 1-2, 7-10; paragraphs [0042]-[0045], [0055], [0064], [0100]-[0105], [0113]-[0146], [0156]-[0175], [0192], [0199]-[0200], [0204]-[0209], [0265]-[0268], [0277]-[0289], [0292]-[0307]	1-31
X	WO 2016029119 A1 (MYVBO LLC [US]) 25 February 2016 (25.02.2016) abstract; Figs. 1-4; pages 1-9	1, 10-11, 13, 22-23, 25-31

☒ 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
30 June 2016 (30.06.2016)	01 July 2016 (01.07.2016)

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
Yrjö Raivio
Telephone No. +358 9 6939 500

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2016/050187

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2015294308 A1 (PAUKER MATTHEW [US] et al.) 15 October 2015 (15.10.2015) abstract; Figs. 3-7, 9; paragraphs [0005]-[0008], [0025], [0032]-[0053], [0058]-[0061]	1-31
A	WO 2016015041 A1 (BLOCKCHAIN TECHNOLOGIES CORP [US]) 28 January 2016 (28.01.2016) abstract; Figs. 1-5; paragraphs [0007]-[0010], [0015], [0028]-[0052]	1-31
A	US 2015371224 A1 (LINGAPPA PHANEENDRA RAMASESHU [US]) 24 December 2015 (24.12.2015) abstract; Figs. 1, 3; paragraphs [0003]-[0011], [0032], [0058]-[0062], [0077]-[0099]	1-31
A	US 2015310424 A1 (MYERS MICHAEL [US]) 29 October 2015 (29.10.2015) abstract; Figs. 1-3, 10; paragraphs [0002]-[0007], [0016]-[0020], [0037]-[0039], [0048]-[0054], [0072]	1-31
A	BARBER, S et al. Bitter to Better - How to Make Bitcoin a Better Currency [online]. Volume 7397 of the series Lecture Notes in Computer Science. Springer Berlin Heidelberg, February 27 - March 02, 2012 [retrieved on 2016-06-23]. Retrieved from the Internet: <URL: http://link.springer.com/chapter/10.1007%2F978-3-642-32946-3_29> Chapter: Financial Cryptography and Data Security, pp. 399-414, Online ISBN: 978-3-642-32946-3. The whole document, in particular Section 6.3.	1, 10-11, 13, 22-23, 25-31
A	KING, S and NADAL S. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. Internet Archive, Community Texts [online database], August 2012 [retrieved on 2016-06-23}. Retrieved from the Internet: <URL: https://ia601705.us.archive.org/33/items/PPCoinPaper/ppcoin-paper.pdf>. The whole document.	1-31
A	EVERAERE, P et al. Double Spending Protection for E-Cash Based on Risk Management. ResearchGate [online database], October 2010 [retrieved on 2016-06-27]. Retrieved from the Internet: <URL: https://www.researchgate.net/publication/220905312>. The whole document, in particular Section 4.	1, 10-11, 13, 22-23, 25-31

INTERNATIONAL SEARCH REPORT
Information on Patent Family Members

International application No.
PCT/FI2016/050187

Patent document cited in search report	Publication date	Patent family members(s)	Publication date
US 2015363782 A1	17/12/2015	None	
WO 2016029119 A1	25/02/2016	WO 2015057840 A1	23/04/2015
US 2015294308 A1	15/10/2015	TW 201602933 A WO 2015160565 A1	16/01/2016 22/10/2015
WO 2016015041 A1	28/01/2016	US 2016027229 A1 US 2016028552 A1 WO 2016022864 A2	28/01/2016 28/01/2016 11/02/2016
US 2015371224 A1	24/12/2015	None	
US 2015310424 A1	29/10/2015	None	

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2016/050187

CLASSIFICATION OF SUBJECT MATTER

IPC
H04L 9/08 (2006.01)
H04L 29/06 (2006.01)
G06F 21/64 (2013.01)
G06Q 20/22 (2012.01)
G06Q 20/36 (2012.01)
G06Q 20/38 (2012.01)