



(51) International Patent Classification:

G06Q 20/02 (2012.01) G06Q 30/06 (2012.01)
G06Q 20/22 (2012.01)

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.

(21) International Application Number:

PCT/EP2017/063366

(22) International Filing Date:

01 June 2017 (01.06.2017)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

16172521.3 01 June 2016 (01.06.2016) EP

(71) Applicant: **BRAND NEW IDEAS B.V.** [NL/NL];
Langstraat 14, 4661 SE Halsteren (NL).

(72) Inventor: **SCHLEE, Justin**; Gaffel 6, 4617 GD Bergen op Zoom (NL).

(74) Agent: **ENGELFRIET, Arnoud Peter**; c/o ICTRecht B.V., P.O. Box 1514, 5200 BN 's-Hertogenbosch (NL).

(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,

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

Declarations under Rule 4.17:

— as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))

Published:

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

(54) Title: VALIDATING BLOCKCHAIN TRANSACTIONS REGARDING REAL MONEY

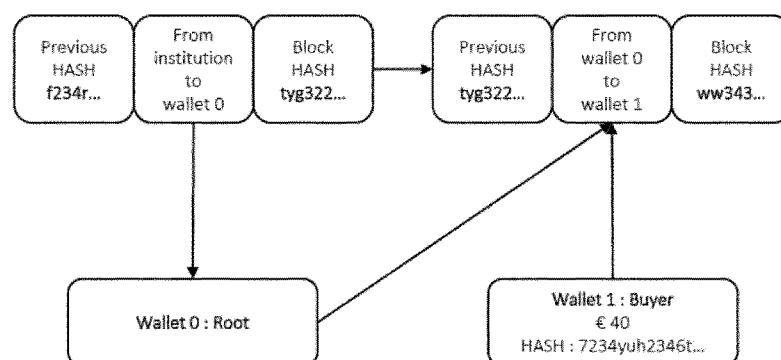


Fig. 3B

(57) Abstract: A computer-implemented method of validating transactions in a blockchain. Transactions comprise a blockchain element indicating a transaction from a seller to a buyer. The transaction is recorded as validated through introduction in the blockchain a further element indicating a receipt by a third party from either the buyer or the seller, said third party being referenced in a root item of the blockchain. Preferably the first blockchain element indicates a transfer from a seller to a buyer and a second blockchain element indicates a receipt by the buyer from the seller. Preferably the third party executes a money transfer operation upon calculating the absence of the further element and upon execution adds the further element.

Validating blockchain transactions regarding real money

FIELD OF THE INVENTION

The invention relates to a computer-implemented method of validating
5 transactions in a blockchain, which transactions comprise a blockchain element indicating a transfer from a seller to a buyer.

The invention further relates to a computer system for implementing the method, a peer-to-peer network, nodes therein and a computer program product.

10 BACKGROUND OF THE INVENTION

Electronic commerce represents a significant part of the world's economy. From selling books to electronic services, almost any item can be bought or sold online. An important challenge in electronic commerce is fraud and other reasons why a transaction may go bad. A seller might not deliver or a buyer might not pay for any
15 number of reasons. Because the parties are not directly interacting with each other as in a classic 'brick and mortar' commercial transaction, this represents a problem that slows down electronic commerce.

Various approaches have been developed to tackle this problem. A classic solution for example is to involve a trusted third party, such as a notary public or an
20 escrow agent. The third party receives the item from the seller and the payment from the buyer, and subsequently transfers both to their intended recipients. This approach is still fraught with problems, as are other business schemes. A more reliable technical solution is therefore desirable.

In 2008, Satoshi Nakamoto (pseudonym) published the paper "Bitcoin: A peer-
25 to-peer electronic cash system." In the paper a cryptographic scheme for facilitating electronic money was proposed, which has proven to be a revolution in the field. Bitcoin represents electronic cash, doing away with a trusted third party and instead employing digital signatures and a peer-to-peer solution for the validation of cash transfers. A network of peers timestamps transactions by hashing them into an ongoing
30 chain of hash-based proof-of-work, the so-called blockchain, forming a record that cannot be changed without redoing the proof-of-work. The blockchain chain thus serves as proof of the sequence of events witnessed.

Over the years, the blockchain technology has been deployed for a great variety of technical applications, including so-called 'smart contracts' and digital asset or

transaction registration. Smart contracts are computer protocols that facilitate, verify, or enforce the negotiation or performance of a contract. In asset or transaction registration, information regarding an asset or transaction is recorded as an item in a blockchain. As the record in a blockchain cannot be changed (under normal circumstances), this thus
5 serves as proof of the correctness of the registered information. Code supporting this is a latent part of the bitcoin protocol, based on probabilistic and anonymous (proof-of-work based) Byzantine replication.

As the present inventor has realized for the first time, one disadvantage of the above applications is that no effective validation of real-world payments can be
10 executed. The Bitcoin scheme enables validated currency transfers in terms of virtual cash, but these must be bought and sold in separate arrangements. Smart contract schemes enable execution and confirmation of contractual arrangements but do not execute the payment itself. There is therefore a need in the art for a technical solution providing validation of real-world payments in a distributed and automated fashion.

15

SUMMARY OF THE INVENTION

To address the above, the invention provides for a computer-implemented method of, and corresponding system for, validating transactions in a blockchain, which transactions comprise a blockchain element indicating a transaction from a seller to a
20 buyer, characterized in that the transaction is recorded as validated through introduction in the blockchain of a further element indicating a receipt by a third party from either the buyer or the seller, said third party being referenced in an initial element or root element of the transaction in the blockchain.

This new further element represents technical information to enable automated
25 calculation of a validation status of the transaction. Transactions are recorded as a sequence of interrelated blockchain elements, said interrelation being effected through use of a common cryptographic hash or other unique identifier for the transaction.

Introducing the further element into the block chain effectively introduces a circle: the item refers to the initial or root element, in an embodiment contains an
30 identifier of the root, and with a simple calculation this circle can be detected by any node in the peer-to-peer network effectuating the blockchain. This detection serves as proof that the transaction has been completed: the goods have been delivered correctly and payment can be made. The calculation serves to execute this validation in an automated manner. Normally, upon detection of the circle a payout is initiated.

Preferably a check is made first if a payment has already been made for this transaction, to avoid double spending.

In an embodiment, the first block (blockchain element) indicates a transfer from a seller to a buyer and a second block (blockchain element) indicates a receipt by the
5 buyer from the seller. This embodiment extends the transaction recordation by employing three items: a first item indicating the delivery of the good or service, a second item indicating receipt of payment and a third item, being the item indicating validation of the transaction through the reference to the root of the transaction.

In another embodiment the third party executes a money transfer operation upon
10 calculating the absence of the further element and upon execution adds the further element. Here the transfer of real-world money is enabled thanks to a technical step: checking for presence or absence of the further element through blockchain validation calculations. If that element is not yet present, i.e. the circle has not yet been found, then the transaction is technically valid. The third party subsequently validates the payment
15 and records the execution thereof. The further element is then added to complete and thereby invalidate the transaction. Due to the validation of the transaction it is now known that this transfer is appropriate (the goods have been delivered) and unique (the transaction will be validated only once). This step becomes possible in an automated technical fashion thanks to the validation of the invention.

20 The invention further advantageously provides for a peer-to-peer network comprising plural nodes, said nodes being configured for validating transactions in a blockchain, which transactions comprise a blockchain element indicating a transaction from a seller to a buyer, one of said nodes being additionally configured for introducing in the blockchain a further element indicating a receipt by a third party from either the
25 buyer or the seller, said third party being referenced in an initial element of the transaction in the blockchain.

The invention further advantageously provides for a node for use with the peer-to-peer network of the invention, being configured for introducing in the blockchain a further element indicating a receipt by a third party from either the buyer or the seller,
30 said third party being referenced in an initial element of the transaction in the blockchain. This node operates as a separate service, e.g. to facilitate the real-world payment, and adds the further element to indicate this has been done.

The invention further advantageously provides for a node for use in the peer-to-peer network of the invention, being configured for causing execution of a money transfer operation upon calculating the absence of the further element.

5 The invention further advantageously provides for a computer-readable storage medium comprising executable code for causing a computer to operate as a peer-to-peer node of the invention.

BRIEF DESCRIPTION OF THE FIGURES

10 The invention will now be explained in more detail with reference to the figures, in which:

Fig. 1 schematically illustrates a peer-to-peer network 100 comprising nodes 101-a...101-n, said nodes being configured for validating transactions in a blockchain;

Fig. 2 schematically illustrates the blockchain aspect of the invention in more detail in the form of a flowchart; and

15 Fig. 3A through 3F illustrate blockchain elements related to steps in the flowchart of Fig. 2.

In the figures, same reference numbers indicate same or similar features. In cases where plural identical features, objects or items are shown, reference numerals are provided only for a representative sample so as to not affect clarity of the figures.

20

DETAILED DESCRIPTION OF CERTAIN EMBODIMENTS

Fig. 1 schematically illustrates a peer-to-peer network 100 comprising nodes 101-a...101-n, said nodes being configured for validating transactions in a blockchain. As such, blockchain networks are well-known in the art and this disclosure will
25 therefore not discuss their implementation in detail. Reference is made to *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* by Andreas M. Antonopoulos (O'Reilly 2015) for a good introductory text. Transactions in this context may refer to any type of transaction in which one item is exchanged for another, typically but not necessarily for money. Items can be physical or digital goods, or items that grant access to online or
30 offline services.

A transaction from a seller to a buyer is recorded in the blockchain as one or more blockchain elements referencing such transaction. The element will include identificational elements of the parties, the transaction itself or both. Identification of either party may be done in any way, as long as the identification is sufficient for the

purpose of the transaction. The transaction may be identified as a single identifier referencing an external record, as a complete summary of the transaction, or any other means of identification as deemed suitable for a particular implementation.

In practice, a hash code is generated to make the transaction element unique. A
5 preferred embodiment therefore is to take the information needed for uniquely identifying the transaction, e.g. an identifier of the seller, an identifier of the buyer and/or a transaction number, and apply a cryptographic hash function such as the well-known SHA-256 algorithm. The outcome is then added to the blockchain as a new element. For purposes of the invention it is preferred that the hash code is calculated
10 from at least a bank account number such as the IBAN of the buyer.

In a preferred embodiment recording the transaction comprises adding first an transaction element representing a step of transferring the item sold from seller to buyer, and second a transaction element representing a step of successfully receiving this item at the buyer. However, a single element representing the transaction as a whole is also
15 possible.

Upon successful receipt of the item, a payment must be made. In accordance with the invention this payment will be effected in a real-world currency from the seller to the buyer. The amount may be recorded in the transaction element.

When the buyer is satisfied with the received item, and payment therefore can be
20 executed, a further element is added to the blockchain. This further element indicates a receipt by a third party from either the buyer or the seller, said third party being referenced in an initial element of the transaction in the blockchain. In this disclosure this third party will also be referred to as an oracle. The third party will typically be a bank or other financial institution that will effectuate the real-world money transfer
25 operation from the buyer to the seller upon calculating the presence of the further element.

The third party will effectuate the money transfer only for a valid transaction. To
The further element creates a circle in the blockchain elements, as the third party is referenced in a root item of the blockchain. This circle can be uniquely identified with
30 known blockchain algorithms. According to the invention, a payout in real-world money can be effected in connection with a transaction if the circle has not yet been detected, or if it has been detected but no payout under that transaction has been registered at the institution. Upon such payout the circle is completed, thus marking the transaction as complete and hence now invalid for future payouts.

Fig. 2 schematically illustrates the blockchain aspect of the invention in more detail in the form of a flowchart. The flowchart assumes an external facility through which a buyer and seller may get in contact with each other to execute a transaction, such as a sale of a physical or digital good for a price expressed in real-world money (as
5 opposed to cryptocurrencies such as Bitcoin). This facility is in principle independent of the invention. What matters is that both buyer and seller are able to initiate the creation of elements in the blockchain indicating certain steps in the transaction. They may create such elements themselves, or have a third party perform such creation.

In step 201, a buyer deposits real money with a bank or other financial
10 institution. This institution serves as the above-referenced third-party. In connection with a transaction to which the deposit relates, the institution supplies to the buyer a unique identifier, such as a hashcode, for the transaction. This identifier will be used as a reference. As an example, identifier 7234yuh2346t will be used. Note that the identifier can be supplied in response to the deposit but could also be issued earlier, e.g.
15 upon an indication of the buyer or the seller that a transaction is about to occur. In step 202, the institution stores information regarding the transaction, including the hash code, in an internal database. This allows for authoritative validation of the information.

In step 203, the institution adds an element to the blockchain, which element refers to the transaction and therefore includes identifier 7234yuh2346t. Preferably, the
20 blockchain implementation is configured such that only the institution can add elements. Alternatively, the institution may digitally sign or otherwise certify elements in order to allow others to identify the elements as originating with the institution. In cryptocurrency terms, the money is put into the wallet of the institution, this is wallet 0.

An example of such an element is shown in Fig. 3A. This element or block
25 contains hashes of previous and next elements and identifies the transaction with identifier 7234yuh2346t. In the example, additional information on the transaction is included in the form of a value of the payment by the buyer, 40 Euros.

In step 204, a new element is added that indicates a transfer of money to the buyer, this is wallet 1. Before this transaction is executed the blockchain software will
30 check the previous transactions and validate the transaction if the money is really available with the institution. An example of the element providing for the transfer is shown in Fig. 3B. If the check is negative, the method instead proceeds to step 220.

In step 205, the transaction between the buyer and seller is recorded. Again, before this transaction is executed the blockchain software will check the previous

transactions and validate the transaction if the money is really available with the institution. In cryptocurrency terms, the money has been transferred from wallet 1 to wallet 2, as shown in Fig. 3C.

In step 207, a transfer between seller and institution is illustrated. Here, the
5 seller wants to receive the money in real currency, which can be provided by the institution as this money has been received in step 201. To execute this transfer, the seller transfers the digital money to wallet 0, associated with the institution. This is illustrated in Fig. 3D.

In step 208 a payment of the example amount of 40 Euros to the seller is
10 executed. To complete this payment, an element is added that indicates a receipt by a third party, the institution, from either the buyer or the seller. This element said third party being referenced in a root item of the blockchain, i.e. the item in Fig. 3A. With this element, a loop is now present in the transaction elements. The transaction started in Fig. 3A originating from the root item, i.e. the institution, and in Fig. 3E that same
15 transaction returns to the root item. This loop indicates the payment has been completed. A later request on payout on this transaction, e.g. as per step 206, will not be accepted.

In step 220, the method deals with situations where after step 204, the buyer finds something is amiss with the transaction. For example, the goods never arrived, or
20 they are faulty. In such a case, the buyer would want to cancel the transaction so as to prevent a payout to the seller. This means that step 205 in the above process must not occur, so that the element of Fig. 3C is not added. Instead, an alternate element is added in step 220, as per Fig. 3F. Here the money is transferred from wallet 1 (buyer) to wallet 0 (root). Next, the method executes payout as per step 208 but this time the money is
25 paid back to the buyer.

CLOSING NOTES

The above provides a description of several useful embodiments that serve to illustrate and describe the invention. The description is not intended to be an exhaustive
30 description of all possible ways in which the invention can be implemented or used. The skilled person will be able to think of many modifications and variations that still rely on the essential features of the invention as presented in the claims. In addition, well-known methods, procedures, components, and circuits have not been described in detail.

Some or all aspects of the invention may be implemented in a computer program product, i.e. a collection of computer program instructions stored on a computer readable storage device for execution by a computer. The instructions of the present invention may be in any interpretable or executable code mechanism, including but not
5 limited to scripts, interpretable programs, dynamic link libraries (DLLs) or Java classes. The instructions can be provided as complete executable programs, as modifications to existing programs or extensions (“plugins”) for existing programs. Moreover, parts of the processing of the present invention may be distributed over multiple computers or processors for better performance, reliability, and/or cost.

10 Storage devices suitable for storing computer program instructions include all forms of non-volatile memory, including by way of example semiconductor memory devices, such as EPROM, EEPROM, and flash memory devices, magnetic disks such as the internal and external hard disk drives and removable disks, magneto-optical disks and CD-ROM disks. The computer program product can be distributed on such a
15 storage device, or may be offered for download through HTTP, FTP or similar mechanism using a server connected to a network such as the Internet. Transmission of the computer program product by e-mail is of course also possible.

When constructing or interpreting the claims, any mention of reference signs shall not be regarded as a limitation of the claimed feature to the referenced feature or
20 embodiment. The use of the word “comprising” in the claims does not exclude the presence of other features than claimed in a system, product or method implementing the invention. Any reference to a claim feature in the singular shall not exclude the presence of a plurality of this feature. The word “means” in a claim can refer to a single means or to plural means for providing the indicated function.

Claims

1. A computer-implemented method of validating transactions in a blockchain, which transactions comprise a blockchain element indicating a transaction
5 from a seller to a buyer, characterized in that the transaction is recorded as validated through introduction in the blockchain of a further element indicating a receipt by a third party from either the buyer or the seller, said third party being referenced in a root item of the blockchain.
- 10 2. The method of claim 1, in which the first blockchain element indicates a transfer from a seller to a buyer and a second blockchain element indicates a receipt by the buyer from the seller.
- 15 3. The method of claim 1, in which the third party executes a money transfer operation upon calculating the absence of the further element and upon execution adds the further element.
- 20 4. A computer system for validating transactions in a blockchain, which transactions comprise a blockchain element indicating a transaction from a seller to a buyer, characterized by validation means for recording the transaction as validated through introduction in the blockchain of a further element indicating a receipt by a third party from either the buyer or the seller, said third party being referenced in a root item of the blockchain.
- 25 5. A peer-to-peer network comprising plural nodes, said nodes being configured for validating transactions in a blockchain, which transactions comprise a blockchain element indicating a transaction from a seller to a buyer, one of said nodes being additionally configured for introducing in the blockchain a further element indicating a receipt by a third party from either the buyer or the seller, said third party
30 being referenced in a root item of the blockchain.
6. A node for use with the peer-to-peer network of claim 5, being configured for introducing in the blockchain a further element indicating a receipt by a

third party from either the buyer or the seller, said third party being referenced in a root item of the blockchain.

7. A node for use with the peer-to-peer network of claim 5, being
5 configured for causing execution of a money transfer operation upon calculating the absence of the further element and upon execution adding the further element.

8. A computer-readable storage medium comprising executable code for causing
a computer to operate as the node of claim 6 or 7.

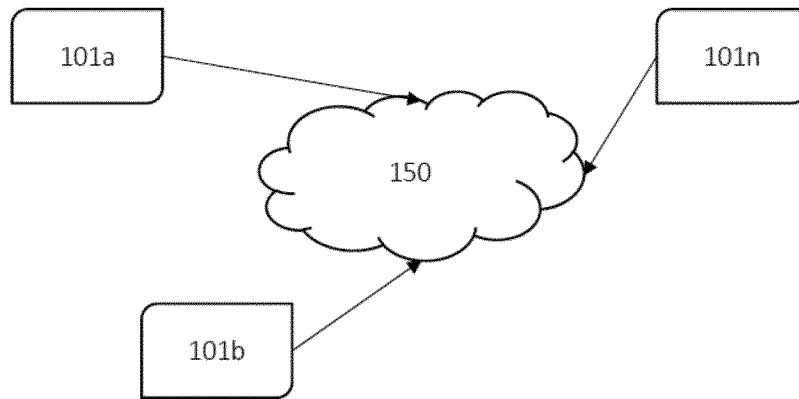


Fig. 1

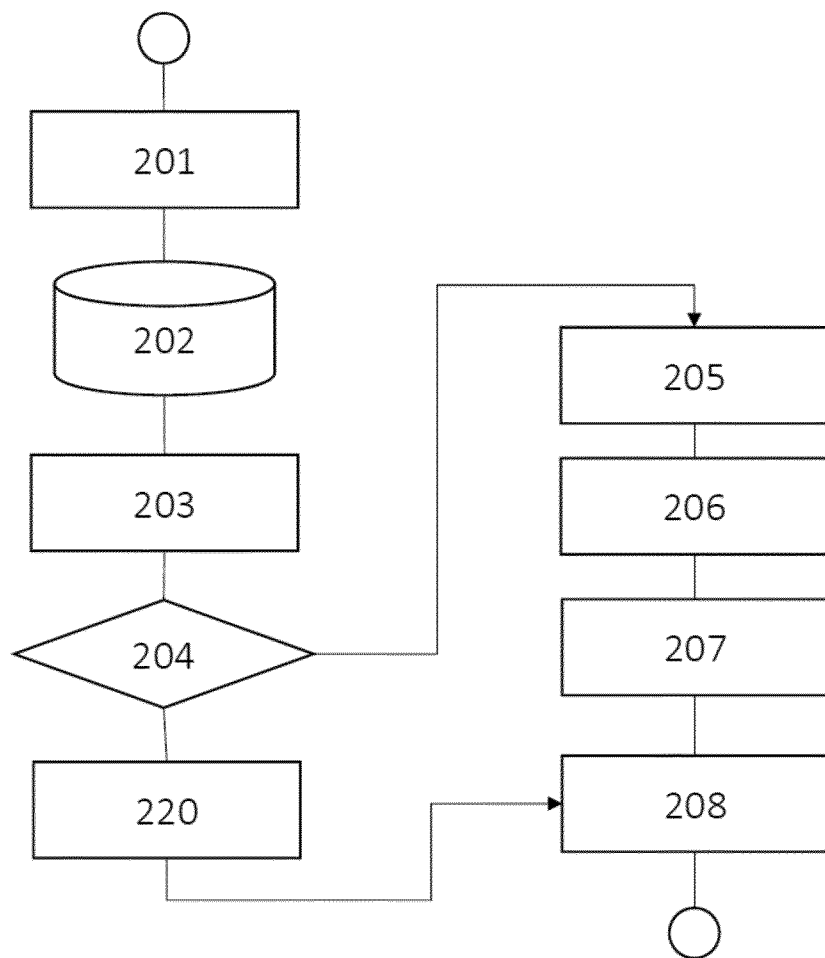


Fig. 2

2/4

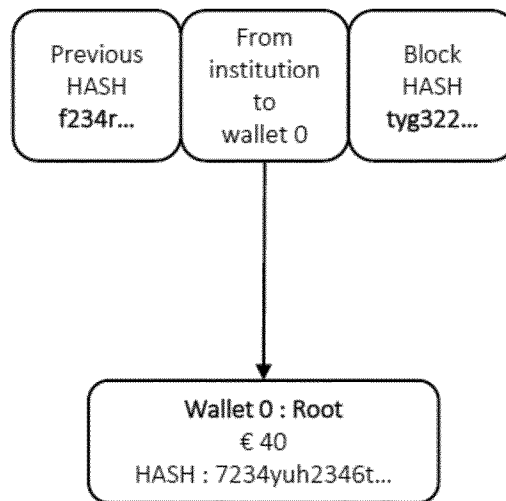


Fig. 3A

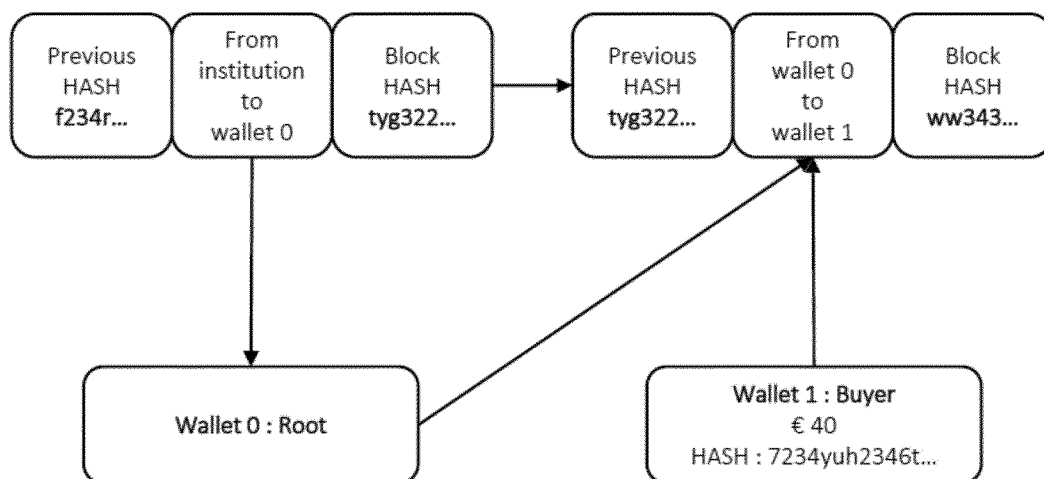


Fig. 3B

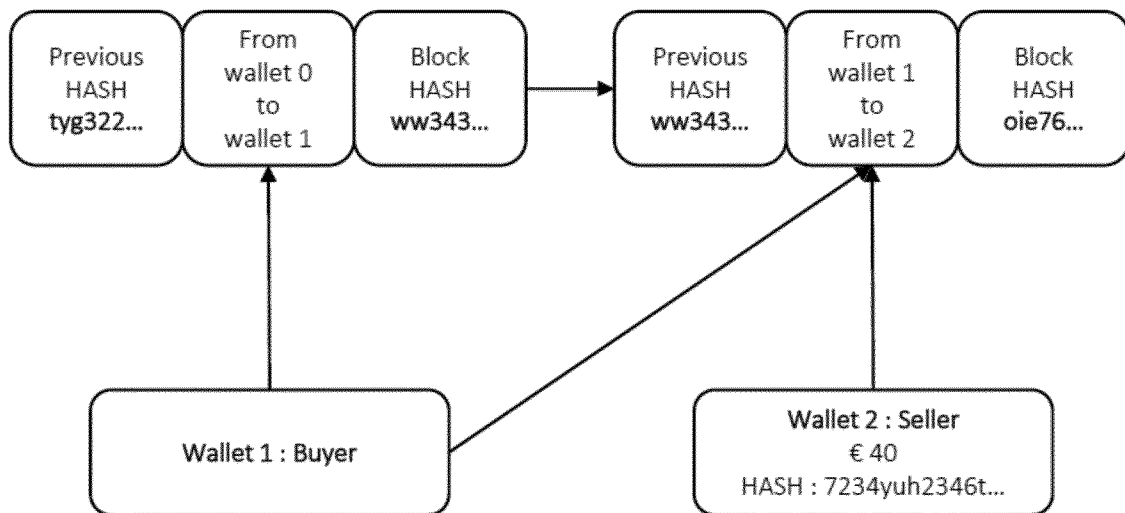


Fig. 3C

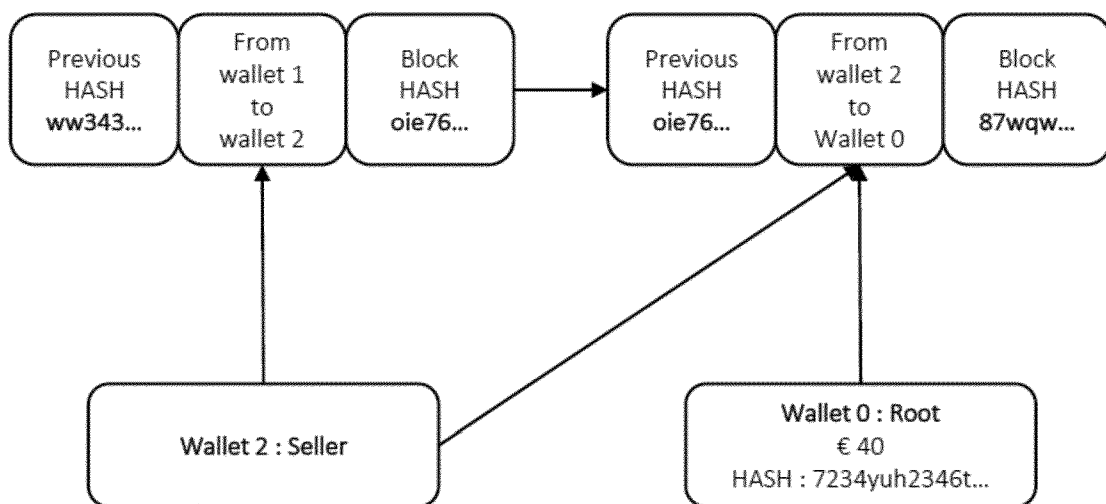


Fig. 3D

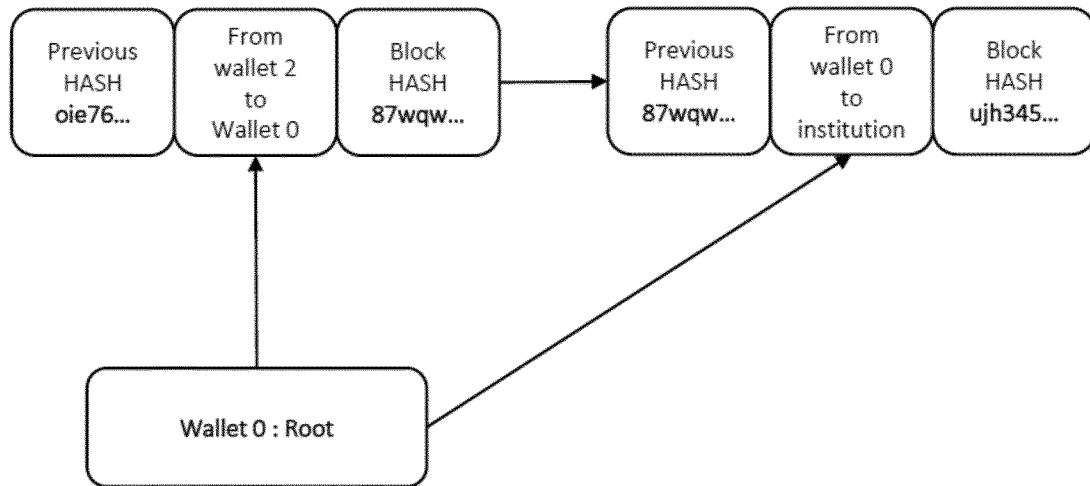


Fig. 3E

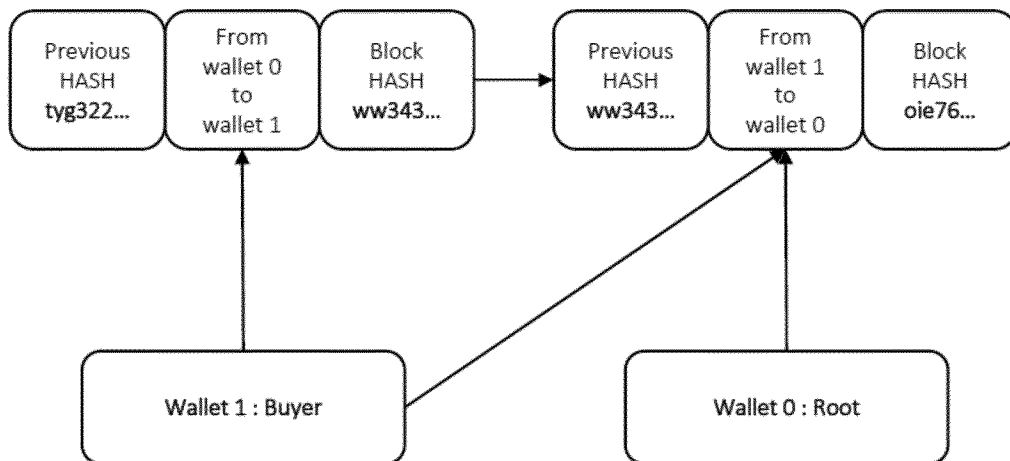


Fig. 3F

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2017/063366

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06Q20/02 G06Q20/22 G06Q30/06
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q H04L

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

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

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2015/356524 A1 (PENNANEN ANTTI [FI]) 10 December 2015 (2015-12-10) the whole document	1-8
X	US 2015/206106 A1 (YAGO YARON EDAN [US]) 23 July 2015 (2015-07-23) paragraph [0042] - paragraph [0067]; figures 1-5	1-8
X	US 2015/269539 A1 (MACGREGOR ROBERT SCOTT [CA] ET AL) 24 September 2015 (2015-09-24) paragraph [0018] - paragraph [0114]; figures	1-8



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

17 July 2017

Date of mailing of the international search report

26/07/2017

Name and mailing address of the ISA/

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

Authorized officer

Blackley, William

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2017/063366

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2015356524 A1	10-12-2015	NONE	
US 2015206106 A1	23-07-2015	US 2015206106 A1 WO 2015106285 A1	23-07-2015 16-07-2015
US 2015269539 A1	24-09-2015	NONE	