



(51) International Patent Classification:

G06Q 20/06 (2012.01) H04L 29/06 (2006.01)

(21) International Application Number:

PCT/CN2018/111368

(22) International Filing Date:

23 October 2018 (23.10.2018)

(25) Filing Language:

English

(26) Publication Language:

English

(71) Applicant: **BEIJING DIDI INFINITY TECHNOLOGY AND DEVELOPMENT CO., LTD** [CN/CN]; Building 34, No. 8 Dongbeiwang West Road, Haidian District, Beijing 100193 (CN).

(72) Inventors: **LIANG, Chuan**; Building 34, No. 8 Dongbeiwang West Road, Haidian District, Beijing 100193 (CN). **YANG, Mengke**; Building 34, No. 8 Dongbeiwang West Road, Haidian District, Beijing 100193 (CN). **LIU, Cunsheng**; Building 34, No. 8 Dongbeiwang West Road, Haidian District, Beijing 100193 (CN).

(74) Agent: **METIS IP (CHENGDU) LLC**; Room 808, 8th Floor, Building B7, Block D, Tianfu Jingrong Center, No. 99 West Section of Hupan Road, Tianfu New District, Chengdu, Sichuan 610213 (CN).

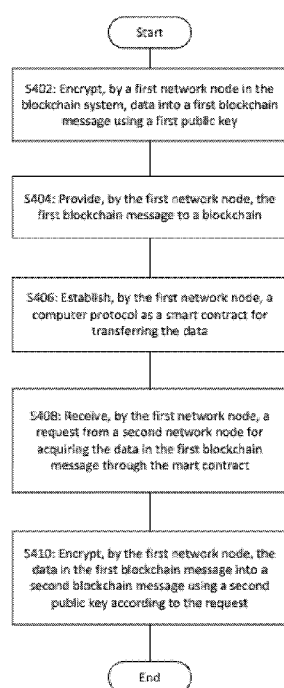
(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Published:

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

(54) Title: METHOD AND SYSTEM FOR TRANSFERRING DATA IN A BLOCKCHAIN SYSTEM



(57) Abstract: Embodiments of the disclosure provide a method and a system for transferring data in a blockchain system. The method can include: encrypting, by a first network node in the blockchain system, the data into a first blockchain message using a first public key; providing, by the first network node, the first blockchain message to a blockchain; establishing, by the first network node, a computer protocol as a smart contract for transferring the data; receiving, by the first network node, a request from a second network node in the blockchain system for acquiring the first blockchain message; and encrypting, by the first network node, the data in the first blockchain message into a second blockchain message using a second public key according to the request.

METHOD AND SYSTEM FOR TRANSFERRING DATA IN A BLOCKCHAIN SYSTEM

TECHNICAL FIELD

5 [0001] The present disclosure relates to blockchain technologies and, more particularly, to methods and systems for transferring data in a blockchain system.

BACKGROUND

10 [0002] A blockchain may be used for storing and sharing data due to the nature of a shared ledger system in the blockchain. The shared ledger system of the blockchain can be used for exchanging data between blockchain users. To protect data, the blockchain generally uses a key encryption scheme (e.g., an asymmetric key encryption scheme) to encrypt the data. For example, data can be encrypted and stored on the blockchain using a public key. And the stored data can be decrypted using a private key corresponding to the public key.

15 [0003] Conventionally, the blockchain can assign a pair of public and private keys to a network node, so that the network node can use the public key to encrypt data and use the private key to decrypt the data. However, the private key is private to each network node. Thus, when a first network node encrypts data using a public key, the encrypted data can be decrypted by a second network node only if the second network node has the private key that
20 is assigned to the first network node. Due to the private nature of the private key, the blockchain cannot allow the first network node to share the private key with the second network node. To exchange the data, the first network node has to share the private key with the second network node off the blockchain. However, sharing the private key off the blockchain can be a security breach to the blockchain, and the exchanging may be inefficient.

25 [0004] To address the above problem, embodiments of the disclosure provide methods and systems for sharing data on a blockchain, so that data exchange can be fully performed on the blockchain.

SUMMARY

30 [0005] Embodiments of the disclosure provide a computer-implemented method for transferring data in a blockchain system. The method can include: encrypting, by a first network node in the blockchain system, the data into a first blockchain message using a first public key; providing, by the first network node, the first blockchain message to a blockchain; establishing, by the first network node, a computer protocol as a smart contract for

transferring the data; receiving, by the first network node, a request of a second network node in the blockchain system for acquiring the data in the first blockchain message through the smart contract; and encrypting, by the first network node, the data in the first blockchain message into a second blockchain message using a second public key according to the request.

- 5 **[0006]** Embodiments of the disclosure further provide a network node in a blockchain system. The network node can include: a processor; a communication interface coupled to the processor and configured to communicate with the blockchain system; and a memory coupled to the processor and storing instructions executable by the processor. The processor is configured to: encrypt data into a first blockchain message using a first public key; provide
10 the first blockchain message to a blockchain; establish a computer protocol as a smart contract for transferring the data; receive a request from a second network node in the blockchain system for acquiring the data in the first blockchain message through the smart contract; and encrypt the data in the first blockchain message into a second blockchain message using a second public key according to the request.
- 15 **[0007]** Embodiments of the disclosure also provide a non-transitory computer-readable medium that stores instructions that, when executed by a processor of a network node in a blockchain system, cause the network node to perform a method for transferring data in the blockchain system. The method can include: encrypting the data into a first blockchain message using a first public key; providing the first blockchain message to a blockchain;
20 establishing a computer protocol as a smart contract for transferring the data; receiving a request from a second network node in the blockchain system for acquiring the data in the first blockchain message through the smart contract; and encrypting the data in the first blockchain message into a second blockchain message using a second public key according to the request.
- 25 **[0008]** It is to be understood that both the foregoing general description and the following detailed description are exemplary and explanatory only and are not restrictive of the invention, as claimed.

BRIEF DESCRIPTION OF THE DRAWINGS

- 30 **[0009]** FIG. 1 illustrates a schematic diagram of a blockchain system, according to an exemplary embodiment of the disclosure.
- [0010]** FIG. 2 illustrates a schematic diagram of a network node in a blockchain system, according to an exemplary embodiment of the disclosure.

[0011] FIG. 3 illustrates a schematic diagram of interactions between network nodes, according to an exemplary embodiment of the disclosure.

[0012] FIG. 4 illustrates a flowchart of a computer-implemented method for transferring data in a blockchain system, according to an exemplary embodiment of the disclosure.

5

DETAILED DESCRIPTION

[0013] Reference will now be made in detail to the exemplary embodiments, examples of which are illustrated in the accompanying drawings. Wherever possible, the same reference numbers will be used throughout the drawings to refer to the same or like parts.

10 [0014] FIG. 1 illustrates a schematic diagram of a blockchain system 100, according to an exemplary embodiment of the disclosure. A blockchain can be typically managed by a decentralized peer-to-peer network, including a plurality of network nodes. As shown in FIG. 1, for example, blockchain system 100 may include a chain of blocks 120 and network nodes 102-110 connected with chain of blocks 120. Network nodes 102-110 can collectively
15 manage chain of blocks 120. Chain of blocks 120 can include a block 122, a block 124, a block 126, and the like. Each block can include a cryptographic hash of the previous block, a timestamp, and stored data. Chain of blocks 120 can be used as a distributed ledger to record data (e.g., transaction data) across network nodes 102-110. In other words, each of network nodes 102-110 can have a copy of the ledger recording the data.

20 [0015] Blockchain system 100 can be a public blockchain, a private blockchain, or a consortium blockchain. The public blockchain (Bitcoin, Ethereum, or the like) can allow any network node to join the blockchain. The private blockchain is controlled by a single administrator, and only sends invitations to selected network nodes as participants having limited accesses. The consortium blockchain, instead of being controlled by a single
25 administrator, can be operated by a group of organizations (e.g., financial institutions).

[0016] Blockchain system 100 can run a smart contract, which is software that can be fully or partially executed without human interaction. For example, a smart contract may be a computer protocol configured to digitally facilitate, verify, or enforce the negotiation or performance of a contract. Also for example, two parties can program agreed terms into a
30 smart contract, and when the terms are met, the smart contract can be automatically executed. It is appreciated that, as each network node in blockchain system 100 holds a copy of the blockchain, the copies of the smart contract may also be distributed across all network nodes.

[0017] In some embodiments, a network node can share data with other network nodes of blockchain system 100. The data can be encrypted and shared for free or for a price (e.g., a

token issued by blockchain system 100). For example, when a network node 102 joins the blockchain system 100, blockchain system 100 can assign network node 102 with a pair of public and private keys. The pair of public and private keys can comply with, e.g., X.509 certificate of a public key infrastructure (PKI). The public key can be used to encrypt the data and publish the encrypted data in blockchain system 100. The encrypted data can also include price information indicating a price for acquiring the data. It is appreciated that, network node 102 can be assigned with a plurality of pairs of public and private keys. Therefore, first data and second data separately uploaded by network node 102 can be encrypted and decrypted using at least one pair of keys, and the at least one pair of keys can be same or different.

[0018] FIG. 2 illustrates a schematic diagram of a network node, e.g., network node 102 (FIG. 1), in a blockchain system, according to an exemplary embodiment of the disclosure. Network node 102 can include a communication interface 202, a memory 204, and a processor 206.

[0019] In exemplary embodiments, communication interface 202 may be in communication with a blockchain such as chain of blocks 120 (Fig. 1). For example, communication interface 202 can be configured to exchange data with the blockchain, including uploading and receiving the data. The uploaded data can be encrypted and stored on the blockchain by network node 102. Communication interface 202 can also be configured to receive a request of another network node, for acquiring the encrypted data. In some embodiments, communication interface 202 can be an integrated services digital network (ISDN) card, cable modem, satellite modem, or a modem to provide a data communication connection. As another example, communication interface 202 can be a local area network (LAN) card to provide a data communication connection to a compatible LAN. Wireless links can also be implemented by communication interface 202. In such an implementation, communication interface 202 can send and receive electrical, electromagnetic or optical signals that carry digital data streams representing various types of information via a network. The network can typically include a cellular communication network, a Wireless Local Area Network (WLAN), a Wide Area Network (WAN), or the like.

[0020] In some embodiments, encrypted data can be uploaded to the blockchain system by a first network node (e.g., network node 102). The encrypted data can also be referred to as a first blockchain message. The first blockchain message can include any data that can be acquired by other network nodes. For example, the data can include a report, experimental data, an e-book, and the like. It is appreciated that data can also be uploaded to the blockchain as plaintext. In some embodiments, the first blockchain message can further include an

abstract in plaintext that is unencrypted information, so that any network node in the blockchain system can review the abstract without acquiring the private key corresponding to the first blockchain message.

[0021] In exemplary embodiments, memory 204 may be configured to store a set of instructions. When the set of instructions is executed by processor 206, processor 206 can perform the data transferring method described in this disclosure. Memory 204 may be implemented as any type of volatile or non-volatile memory devices, or a combination thereof, such as a static random access memory (SRAM), an electrically erasable programmable read-only memory (EEPROM), an erasable programmable read-only memory (EPROM), a programmable read-only memory (PROM), a read-only memory (ROM), a magnetic memory, a flash memory, or a magnetic or optical disk.

[0022] In exemplary embodiments, processor 206 may include multiple modules, such as an encryption unit 2062, a smart contract unit 2064, and a decryption unit 2066. These modules (and any corresponding sub-modules or sub-units) can be functional hardware units (e.g., portions of an integrated circuit) of processor 206 designed for use with other components or a part of a program (stored on a computer-readable medium) that, when executed by processor 206, performs one or more functions.

[0023] Although FIG. 2 shows units 2062-2066 all within one processor 206, it is contemplated that these units may be distributed among multiple processors located near or remotely with each other.

[0024] In exemplary embodiments, encryption unit 2062 can encrypt data into a first blockchain message using a first public key. As noted above, blockchain system 100 (FIG. 1) can assign each of the network nodes (e.g., network nodes 102 and 104) with a pair of keys, including a public key and a private key. In some embodiments, a random number generator can generate a serial of random numbers. And a key generator can generate the pair of keys based on the serial of random numbers. Based on the public key, plaintext data can be converted to ciphered data. Then, the first blockchain message can be uploaded to blockchain 120 using communication interface 202.

[0025] In exemplary embodiments, smart contract unit 2064 can establish a smart contract for transferring the data. Smart contract unit 2064 can set up terms for acquiring the data in the smart contract, such a price for the data, a condition for triggering a token transfer, and the like.

[0026] As described above, the first blockchain message can include an abstract of the data in plaintext. Therefore, any other network node (e.g., network node 104) can review the

abstract without decrypting the message. For example, if network node 104 finds the data associated with the abstract worth acquiring, network node 104 can send out a request to the smart contract. In some embodiments, the first blockchain message can further include the terms of the smart contract in plaintext, so that network nodes can understand the terms of the smart contract.

[0027] Upon receiving the request of network node 104, smart contract unit 2064 can further generate a transfer event in the smart contract for transferring the data to network node 104. As discussed above, two parties, for example, can program agreed terms into the smart contract and allow automatic execution of the smart contract. When network node 104 sends out the request, the smart contract deems that network node 104 agrees on the terms of network node 102 and therefore programs the terms into the transfer event. It is appreciated that, after the transfer event has been generated, the smart contract can continuously monitor each step of the data transfer. Smart contract unit 2064 can forward the request of network node 104 to network node 102. Accordingly, network node 102 can receive the request of network node 104 for acquiring the first blockchain message, for example, using communication interface 202.

[0028] In some embodiments, network node 104 also has a pair of a second public key and a second private key. And network node 104 can attach the second public key to the request, so that the request received by network node 102 can include the second public key.

[0029] FIG. 3 illustrates a schematic diagram of interactions between network nodes 102 and 104, according to an exemplary embodiment of the disclosure. For illustrative purposes only, a smart contract is shown in a separate block from network nodes 102 and 104 in FIG. 3. It is appreciated that the smart contract may be a computer protocol implemented in network nodes 102 and 104 or a server separated from network nodes 102 and 104.

[0030] Referring to FIG. 3, at 301, network node 104 can send a request for acquiring the data in the first blockchain message to the smart contract, along with the second public key (not shown). And at 303, the smart contract can forward the request including the second public key to network node 102.

[0031] Upon receiving the request of network node 104, decryption unit 2066 of network node 102 can decrypt the first blockchain message to obtain the original data, using a private key corresponding to the first public key that was used to encrypt the data. The first public key and the corresponding private key can comply with X.509 certificate. Then, encryption unit 2062 can further encrypt the obtained original data into a second blockchain message using the second public key of network node 104. In some embodiments, network node 102

may keep a copy of the original data. Therefore, network node 102 may perform the encryption on the copy of the original data, without decrypting the first blockchain message first to acquire the original data.

[0032] At 305, network node 102 can upload the second blockchain message back onto the blockchain. When the smart contract detects the second blockchain message has been uploaded, the smart contract can notify network node 104 to retrieve the second blockchain message. After network node 104 retrieves the second blockchain message, network node 104 can use its private key corresponding to the second public key to decrypt the second blockchain message, so as to acquire the original data.

[0033] In some embodiments, the agreed terms programmed by smart contract unit 2064 can include, for example, a price for the data, a condition for triggering a token transfer, and the like. The condition for triggering the transaction can be, for example, network node 104 retrieving the second blockchain message. In another example, the condition for triggering the transaction can be network node 104 decrypting the second blockchain message. It is appreciated that the agreed terms can be different according the negotiation between network nodes 102 and 104. The smart contract can monitor if the condition is met. When the condition is met, the smart contract can transfer the agreed price (e.g., tokens) to network node 102 and the data transferring can be complete.

[0034] FIG. 4 illustrates a flowchart of a computer-implemented method 400 for transferring data in a blockchain system, according to an exemplary embodiment of the disclosure. For example, method 400 may be implemented by network node 102 including at least one processor, and may include steps S402-S410 as described below.

[0035] In step S402, network node 102 can encrypt data into a first blockchain message using a first public key. Based on the first public key, plaintext data can be converted to ciphered data. The first blockchain message can include an abstract of the data. The abstract can be unencrypted information in plaintext. Therefore, other network nodes (e.g., a network node 104) can review the abstract without decrypting the message.

[0036] Then, in step S404, network node 102 can provide, e.g., upload, the first blockchain message to a blockchain. As described above, a blockchain can include a plurality of blocks each including a cryptographic hash of the previous block, a timestamp, and stored data.

[0037] In step S406, network node 102 can establish a computer protocol as a smart contract for transferring the data. Network node 102 can set up terms for acquiring the data in the smart contract, such a price for the data, a condition for triggering a token transfer, and the like. In some embodiments, the first blockchain message can further include the above

terms of the smart contract in plaintext, so that other network nodes can understand the terms of the smart contract. If another network node (e.g., network node 104) finds the data associated with the abstract worth acquiring, network node 104 can send out a request to the smart contract.

5 **[0038]** Upon receiving the request of network node 104, the smart contract can further generate a transfer event in the smart contract for transferring the data to network node 104. As discussed above, two parties, for example, can program agreed terms into the smart contract and allow automatically execution of the smart contract. When network node 104 sends out the request, the smart contract deems that network node 104 agrees on the terms of
10 network node 102 and therefore programs the terms into the transfer event. The smart contract can forward the request of network node 104 to network node 102.

[0039] Accordingly, in step S408, network node 102 can receive the request from network node 104 for acquiring the first blockchain message through the smart contract.

[0040] In exemplary embodiments, as discussed above, network node 104 also has a pair
15 of a second public key and a second private key. And network node 104 can attach the second public key to the request, so that the request received by network node 102 can include the second public key.

[0041] Upon receiving the request of network node 104, in step S410, network node 102 can encrypt the first blockchain message into a second blockchain message using the second
20 public key. In some embodiments, network node 102 can decrypt the first blockchain message to obtain the original data, using a private key corresponding to the first public key that was used to encrypt the data. The first public key and the corresponding private key can comply with X.509 certificate. Then, network node 102 can further encrypt the obtained original data into a second blockchain message using the second public key of network node
25 104. In some embodiments, network node 102 may keep a copy of the original data. Therefore, network node 102 may perform the encryption on the copy of the original data, without decrypting the first blockchain message first to acquire the original data.

[0042] Network node 102 can upload the second blockchain message back onto the blockchain. When the smart contract detects the second blockchain message has been
30 uploaded, the smart contract can notify network node 104 to retrieve the second blockchain message. After network node 104 retrieves the second blockchain message, network node 104 can use its private key corresponding to the second public key to decrypt the second blockchain message, so as to acquire the original data.

[0043] As discussed above, in some embodiments, the agreed terms programmed by smart contract unit 2064 can include, for example, a price for the data, a condition for triggering a token transfer, and the like. The condition for triggering the transaction can be, for example, network node 104 retrieving the second blockchain message. In another example, the condition for triggering the transaction can be network node 104 decrypting the second blockchain message. It is appreciated that the agreed terms can be different according the negotiation between network nodes 102 and 104. The smart contract can monitor if the condition is met. When the condition is met, smart contract can transfer the agreed price (e.g., tokens) to network node 102 and the data transferring can be complete.

[0044] Embodiments of the disclosure can further provide a non-transitory computer-readable medium storing instructions which, when executed, cause one or more processors to perform the above described data transferring methods. The computer-readable medium may include volatile or non-volatile, magnetic, semiconductor, tape, optical, removable, non-removable, or other types of computer-readable medium or computer-readable storage devices. For example, the computer-readable medium may be the storage device or the memory module having the computer instructions stored thereon, as disclosed. In some embodiments, the computer-readable medium may be a disc or a flash drive having the computer instructions stored thereon.

[0045] It will be apparent to those skilled in the art that various modifications and variations can be made to the disclosed system and related methods. Other embodiments will be apparent to those skilled in the art from consideration of the specification and practice of the disclosed system and related methods.

[0046] It is intended that the specification and examples be considered as exemplary only, with a true scope being indicated by the following claims and their equivalents.

WHAT IS CLAIMED IS:

1. A computer-implemented method for transferring data in a blockchain system, comprising:
encrypting, by a first network node in the blockchain system, the data into a first
5 blockchain message using a first public key;
providing, by the first network node, the first blockchain message to a blockchain;
establishing, by the first network node, a computer protocol as a smart contract for
transferring the data;
receiving, by the first network node, a request from a second network node in the
10 blockchain system for acquiring the data in the first blockchain message through the smart
contract; and
encrypting, by the first network node, the data in the first blockchain message into a
second blockchain message using a second public key according to the request.
- 15 2. The method of claim 1, further comprising:
the smart contract generating a transfer event for sending the second blockchain message
to the second network node, wherein the transfer event is complete when the second network
node retrieves the second blockchain message and decrypts the second blockchain message
into the data using a private key corresponding to the second public key.
20
3. The method of claim 1, wherein receiving the request comprises receiving the second
public key included in the request from the second network node.
4. The method of claim 1, wherein encrypting the data in the first blockchain message into
25 the second blockchain message using the second public key comprises:
decrypting the first blockchain message to obtain the data; and
encrypting the obtained data into the second blockchain message using the second public
key.
- 30 5. The method of claim 1, further comprising:
including in the first blockchain message an abstract of the data, the abstract being
unencrypted information in plaintext.

6. The method of claim 1, further comprising:
assigning the first public key and a corresponding private key to the first network node.
7. The method of claim 6, wherein the first public key and the corresponding private key
5 comply with X.509 certificate.
8. The method of claim 1, wherein the blockchain is a consortium blockchain.
9. A first network node in a blockchain system, comprising:
10 a processor;
a communication interface coupled to the processor and configured to communicate
with the blockchain system; and
a memory storing instructions executable by the processor,
wherein the processor is configured to:
15 encrypt data into a first blockchain message using a first public key;
provide the first blockchain message to a blockchain;
establish a computer protocol as a smart contract for transferring the data;
receive a request from a second network node in the blockchain system for acquiring
the data in the first blockchain message through the smart contract; and
20 encrypt the data in the first blockchain message into a second blockchain message
using a second public key according to the request.
10. The first network node of claim 9, wherein the smart contract further generates a transfer
event of for sending the second blockchain message to the second network node, wherein
25 the transfer event is complete when the second network node retrieves the second blockchain
message and decrypts the second blockchain message into the data using a private key
corresponding to the second public key.
11. The first network node of claim 9, wherein the processor is further configured to receive
30 the request from the second network node to receive the second public key included in the
request from the second network node.
12. The first network node of claim 9, wherein the processor is further configured to:
decrypt the first blockchain message to obtain the data; and

encrypt the obtained data into the second blockchain message using the second public key.

13. The first network node of claim 9, wherein the processor is further configured to include
5 in the first blockchain message an abstract of the data, the abstract being unencrypted information in plaintext.

14. The first network node of claim 9, wherein the processor is further configured to assign
10 the first public key and a corresponding private key to the first network node.

15. The first network node of claim 14, wherein the first public key and the corresponding private key comply with X.509 certificate.

16. The first network node of claim 9, wherein the blockchain is a consortium blockchain.
15

17. A non-transitory computer-readable medium that stores instructions, when executed by a processor of a network node in a blockchain system, cause the network node to perform a method for transferring data in the blockchain system, the method comprising:

20 encrypting the data into a first blockchain message using a first public key;

providing the first blockchain message to a blockchain;

establishing a computer protocol as a smart contract for transferring the data;

receiving a request from a second network node in the blockchain system for acquiring the data in the first blockchain message through the smart contract; and

25 encrypting the data in the first blockchain message into a second blockchain message using a second public key according to the request.

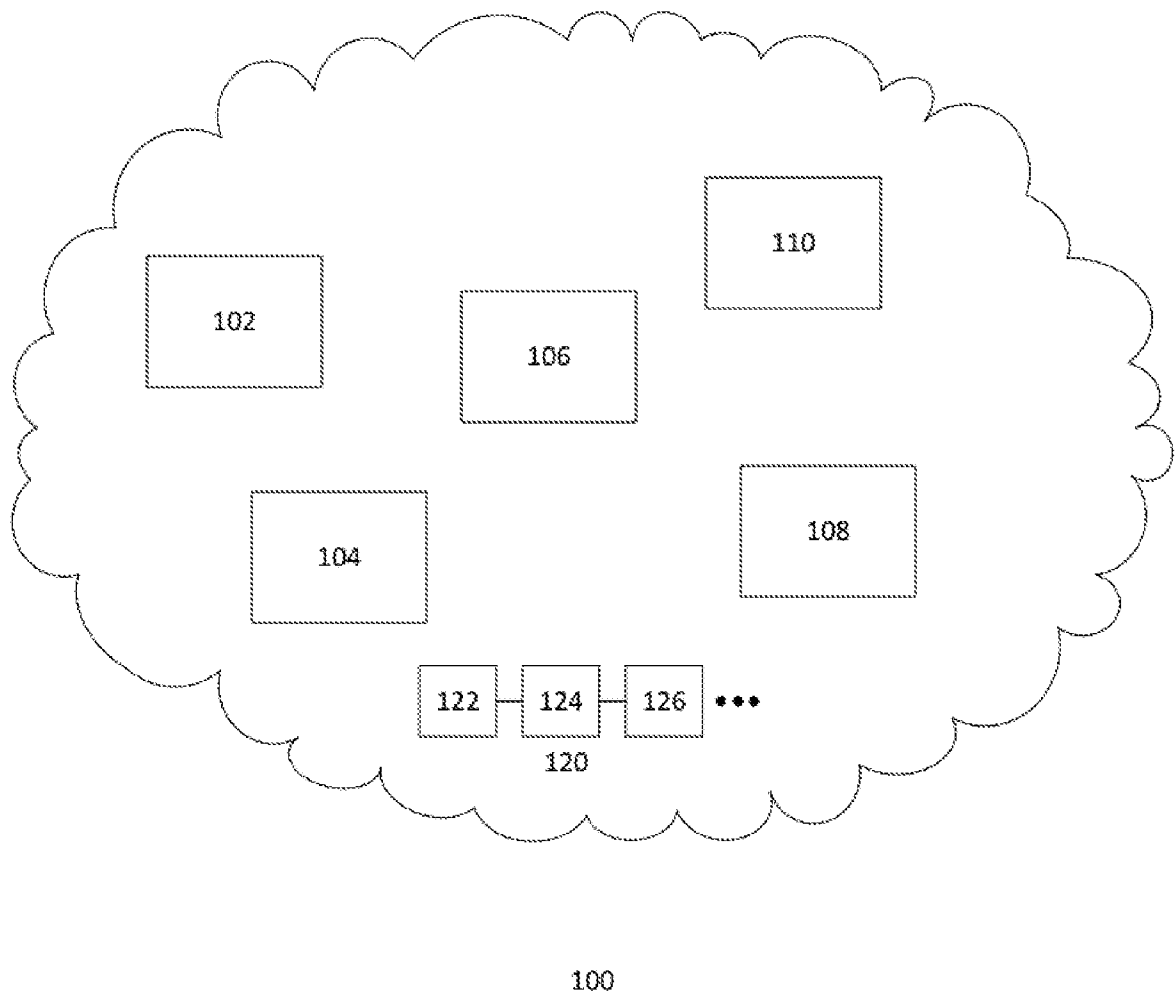


FIG. 1

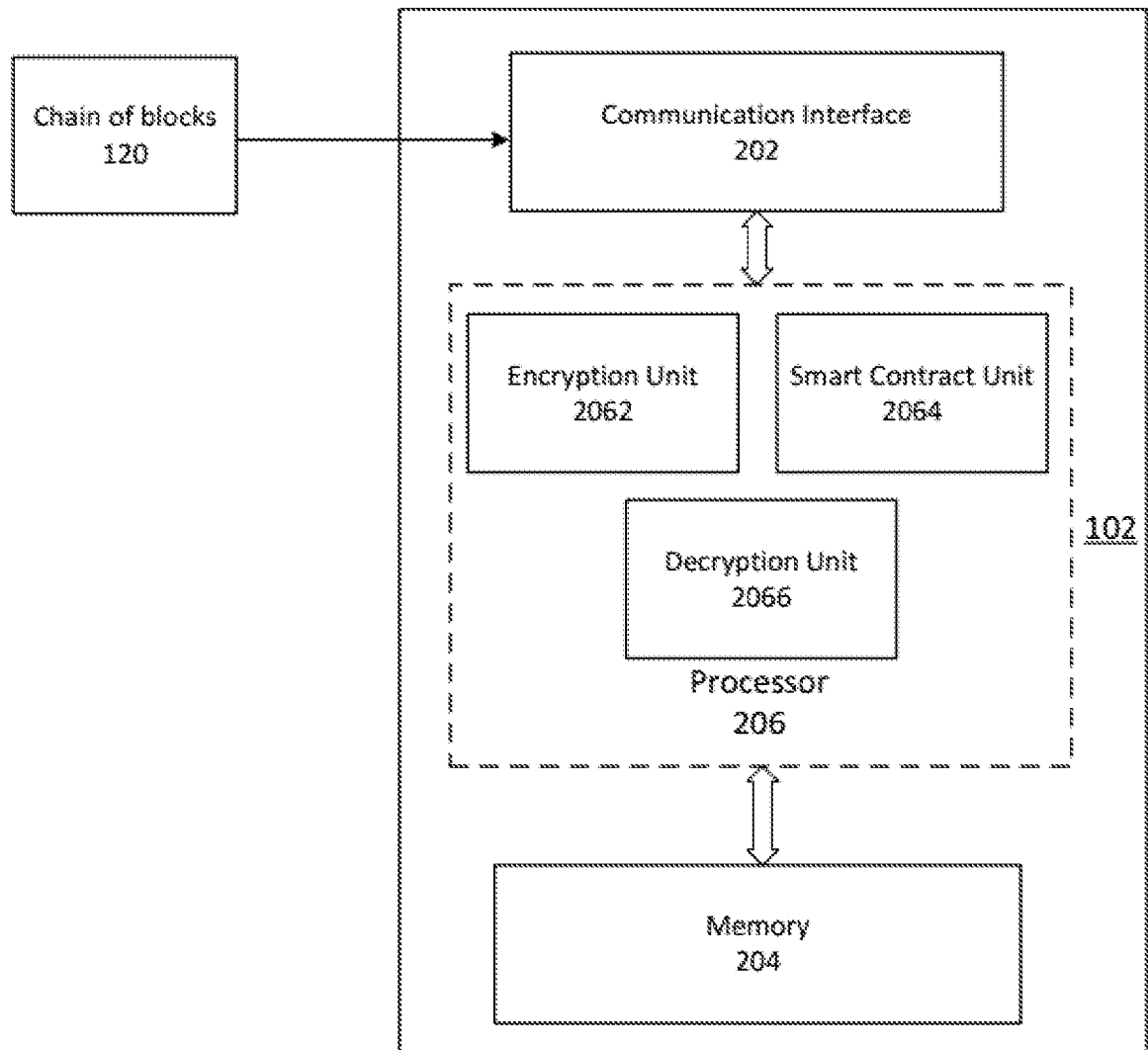


FIG. 2

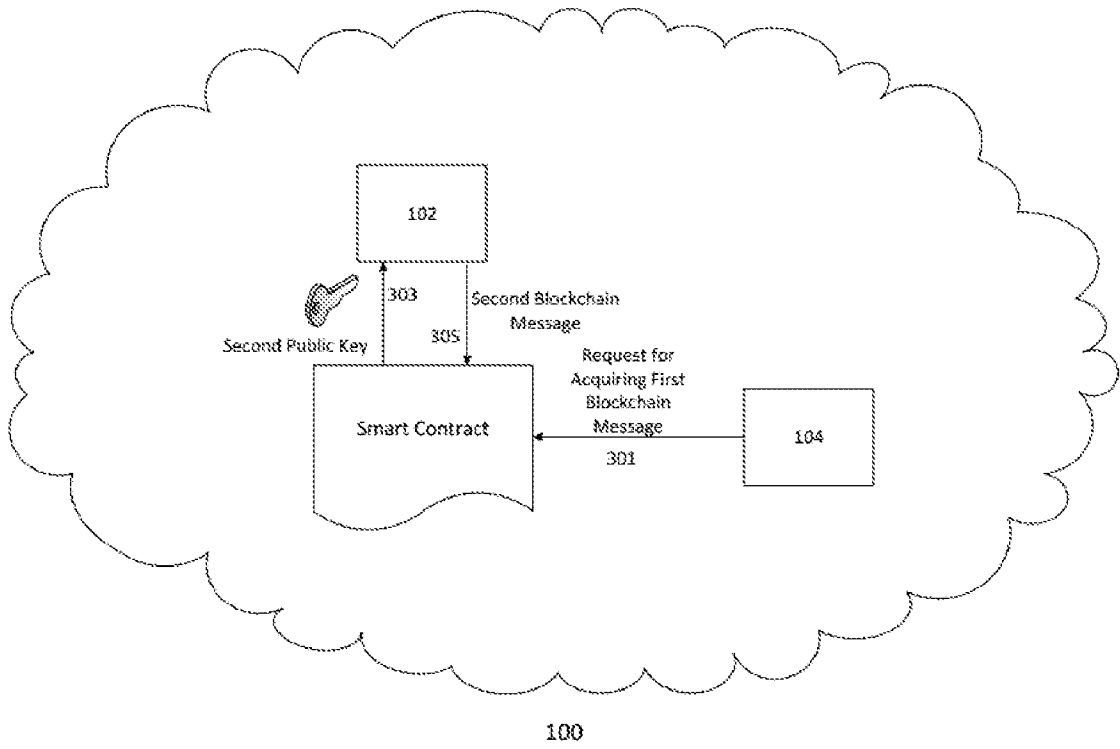
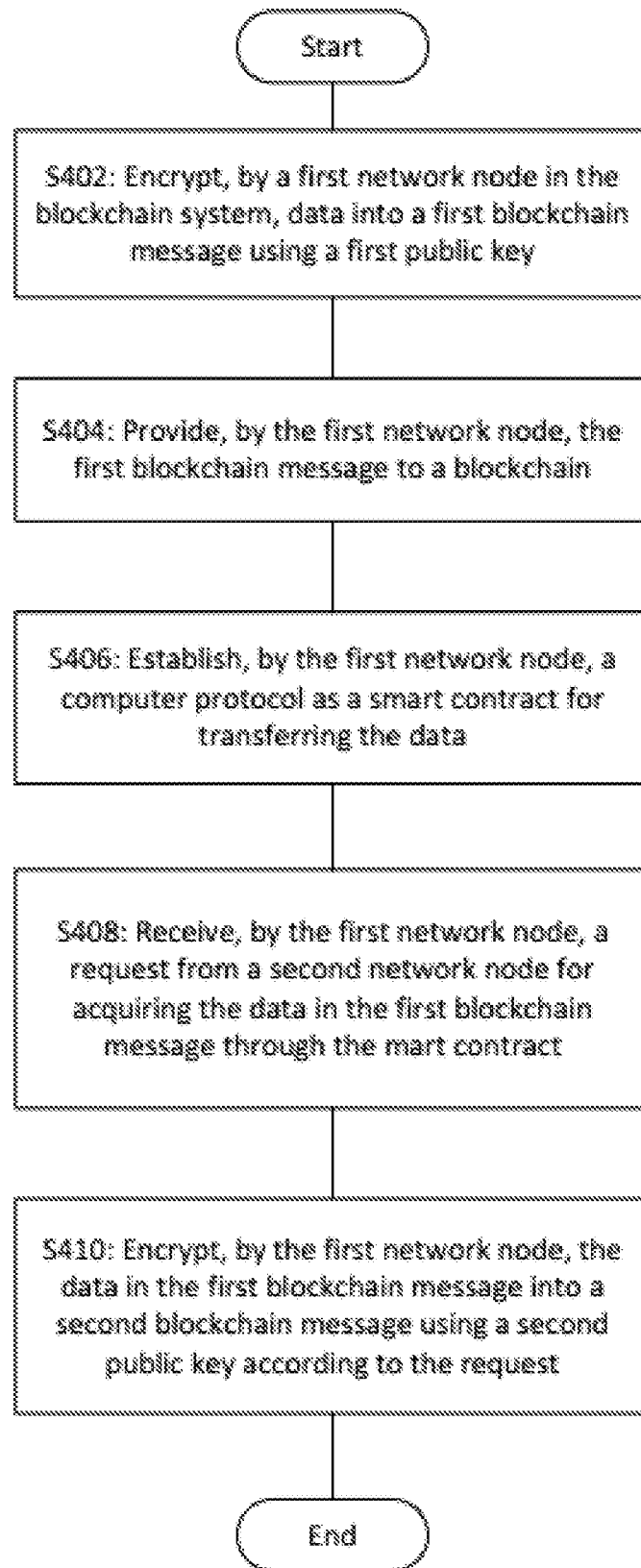


FIG. 3



400

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2018/111368

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/06(2012.01)i; H04L 29/06(2006.01)i

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 G06F 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)

CNPAT, CNKI, WPI, EPODOC: blockchain transfer data smart contract encrypt decrypt public private key abstract

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 107730225 A (GUANGDONG UNIVERSITY OF TECHNOLOGY) 23 February 2018 (2018-02-23) description paragraphs 8-125	1-17
Y	CN 107203344 A (ZHENGZHOU YUNHAI INFORMATION TECHNOLOGY) 26 September 2017 (2017-09-26) description paragraphs 28-49	1-17
A	CN 106100981 A (BUBI BEIJING NETWORK TECHNOLOGY CO., LTD.) 09 November 2016 (2016-11-09) the whole document	1-17
A	US 10057243 B1 (MOCANA CORPORATION) 21 August 2018 (2018-08-21) the whole document	1-17



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

05 July 2019

Date of mailing of the international search report

29 July 2019

Name and mailing address of the ISA/CN

National Intellectual Property Administration, PRC
6, Xitucheng Rd., Jimen Bridge, Haidian District, Beijing
100088
China

Authorized officer

FENG,Nan

Facsimile No. (86-10)62019451

Telephone No. 86-(10)-53961665

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2018/111368

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	107730225	A	23 February 2018	None			
CN	107203344	A	26 September 2017	None			
CN	106100981	A	09 November 2016	None			
US	10057243	B1	21 August 2018	US	10162968	B1	25 December 2018
				US	2019166117	A1	30 May 2019
				WO	2019108438	A1	06 June 2019
				US	2019166116	A1	30 May 2019
				WO	2019108435	A1	06 June 2019