

BLOCK CONTENT EDITING METHODS AND APPARATUSES

TECHNICAL FIELD

[0001] One or more embodiments of the present specification relate to the field of
5 blockchain technologies, and in particular, to block content editing methods and apparatuses.

BACKGROUND

[0002] Blockchain technologies (also referred to as distributed ledger technologies)
are decentralized distributed database technologies, characterized by de-centrality,
10 openness and transparency, tamper-resistance, trustiness, etc., and are applicable to many application scenarios with high demands on data reliability.

SUMMARY

[0003] In view of this, one or more embodiments of the present specification provide block content editing methods and apparatuses.

15 [0004] To achieve the objectives, one or more embodiments of the present specification provide the following technical solutions:

[0005] According to a first aspect of the one or more embodiments of the present specification, a block content editing method is provided, including the following: a blockchain node B_i receives a block editing transaction, which is used to edit original
20 block content m of a block Q_i to target block content m' , wherein a parent hash corresponding to the block Q_i is recorded in a block header of a block Q_{i+1} , the parent hash is generated through calculation by using original block content m , a public key H , and an original random number r , the public key H is generated through calculation by using node public keys h_1 to h_n respectively corresponding to
25 blockchain nodes B_1 to B_n , and $i \in [1, n]$ and i is a positive integer; the blockchain node B_i executes a smart contract that generates a random number when determining that a consensus on the block editing transaction succeeds, wherein the smart contract is used to execute secure multi-party computing related to node private keys x_1 to x_n

respectively corresponding to the blockchain nodes $B1$ to Bn to generate a private key X ; and determine corresponding target random number r' based on the original block content m , the target block content m' , the original random number r , and the private key X , wherein a hash value generated through calculation by using the target block content m' , the public key H , and the target random number r' is the same as the parent hash; and the blockchain node Bi updates the original block content m to the target block content m' and the original random number r to the target random number r' .

[0006] According to a second aspect of the one or more embodiments of the present specification, a block content editing apparatus is provided. The block content editing apparatus can include: a receiving unit, configured to enable a blockchain node Bi to receive a block editing transaction, which is used to edit original block content m of a block Qi to target block content m' , wherein a parent hash corresponding to the block Qi is recorded in a block header of a block $Qi+1$, the parent hash is generated through calculation by using original block content m , a public key H , and an original random number r , the public key H is generated through calculation by using node public keys $h1$ to hn respectively corresponding to blockchain nodes $B1$ to Bn , and $i \in [1, n]$ and i is a positive integer; an execution unit, configured to enable the blockchain node Bi to execute a smart contract, which is used to generate a random number when determining that a consensus on the block editing transaction succeeds, wherein the smart contract is used to execute secure multi-party computing related to node private keys $x1$ to xn respectively corresponding to the blockchain nodes $B1$ to Bn to generate the private key X ; and determine corresponding target random number r' based on the original block content m , the target block content m' , the original random number r , and the private key X , wherein a hash value generated through calculation by using the target block content m' , the public key H , and the target random number r' is the same as the parent hash; and an updating unit, configured to enable the blockchain node Bi to update the original block content m to the target block content m' and the original random number r to the target random number r' .

[0007] According to a third aspect of the one or more embodiments of the present specification, a blockchain node is provided, including: a processor; and a memory configured to store a processor-executable instruction.

[0008] The processor implements the method described in the first aspect by executing the executable instruction.

[0009] According to a fourth aspect of the one or more embodiments of the present specification, a computer-readable storage medium is provided, and the storage medium stores a computer instruction. The steps of the method described in the first aspect are implemented when the instruction is executed by a processor.

5

BRIEF DESCRIPTION OF DRAWINGS

[0010] FIG. 1 is a schematic diagram illustrating a blockchain structure according to an example embodiment;

[0011] FIG. 2 is a flowchart illustrating a block content editing method according to an example embodiment;

10 [0012] FIG. 3 is a schematic diagram illustrating smart contract creation according to an example embodiment;

[0013] FIG. 4 is a schematic diagram illustrating smart contract invocation according to an example embodiment;

15 [0014] FIG. 5 is a schematic structural diagram illustrating a device according to an example embodiment; and

[0015] FIG. 6 is a block diagram illustrating a block content editing apparatus according to an example embodiment.

DESCRIPTION OF EMBODIMENTS

20 [0016] The example embodiments are described in detail here, and examples of the embodiments are shown in the accompanying drawings. When the following description relates to the accompanying drawings, the same numbers in different accompanying drawings indicate the same element or similar elements unless otherwise indicated. The implementations described in the following example embodiments do not represent all implementations consistent with the one or more
25 embodiments of the present specification. On the contrary, they are merely examples of apparatuses and methods consistent with some aspects of the one or more embodiments of the present specification as detailed in the claims.

[0017] It is worthwhile to note that in other embodiments, the steps of the corresponding method are not necessarily performed in the order shown and described
30 in the present specification. In some other embodiments, the method can include more

or fewer steps than the steps described in the present specification. Further, a single step described in the present specification may be divided into multiple steps for description in other embodiments; and multiple steps described in the present specification may be combined into a single step for description in other
5 embodiments.

[0018] A blockchain is formed by chaining several blocks in sequence, and tamper-resistance of content of the blockchain is related to an anchoring relationship between adjacent blocks. FIG. 1 is a schematic diagram illustrating a blockchain structure according to an example embodiment. As shown in FIG. 1, the anchoring
10 relationship is described by taking two blocks with block heights of Q_i and Q_{i+1} as an example. For ease of understanding, a block with the block height of Q_i is referred to as block Q_i , and a block with a block height of Q_{i+1} is referred to as block Q_{i+1} .

[0019] Block Q_i and block Q_{i+1} have the same structure and each includes a block header and a block body. In practice, all blocks have the same structure. A block
15 header of block Q_{i+1} includes information $HASH_Q_i$ shown in FIG. 1. $HASH_Q_i$ is a parent hash included in block Q_{i+1} , and the parent hash $HASH_Q_i$ is obtained by performing a hash operation on content of block Q_i . Because block Q_i and block Q_{i+1} are adjacent blocks and block Q_i is created earlier than block Q_{i+1} , block Q_i can be considered as a parent block of block Q_{i+1} and a hash generated based on the content
20 of block Q_i is referred to as the parent hash. Similarly, if block Q_i also has a corresponding parent block, a block header of block Q_i can also include a parent hash corresponding to the parent block; or if block Q_i is a genesis block, i.e. block Q_i does not have a parent block, the block header of block Q_i does not have to include the parent hash.

[0020] The hash operation can be performed on any input content and a
25 corresponding hash value can be output. In addition, due to the characteristic of the hash operation, it almost can be considered that there is a one-to-one mapping relationship between input content and hash values, and there is only very small probability that a hash collision may occur, i.e. different input content generates the
30 same hash value. In the related technologies, the occurrence probability of the hash collision can be reduced as much as possible in various ways, such as enlarging value space of hash values, so that the hash collision is almost negligible. Therefore, the content of block Q_i can be anchored by including parent hash $HASH_Q_i$ in the block header of block Q_{i+1} . Because a change in the content of block Q_i results in a

different hash value from parent hash $HASH_Q_i$, it is very easy to find that the content of block Q_i is tampered with.

[0021] However, in some applications, for example, private data may be recorded on the blockchain without being encrypted, resulting in a risk of privacy exposure. For another example, erroneous data may be recorded on the blockchain, resulting in a waste of storage space on the blockchain. In conclusion, there is a block content editing need for a chained block. Block content editing solutions provided in the present specification are described below.

[0022] FIG. 2 is a flowchart illustrating a block content editing method according to an example embodiment. As shown in FIG. 2, the method can include the following steps:

[0023] Step 202: Blockchain node B_i receives a block editing transaction, which is used to edit original block content m of block Q_i to target block content m' , wherein a parent hash corresponding to block Q_i is recorded in a block header of block Q_{i+1} , the parent hash is generated through calculation by using original block content m , public key H , and original random number r , public key H is generated through calculation by using node public keys h_1 to h_n respectively corresponding to blockchain nodes B_1 to B_n , and $i \in [1, n]$ and i is a positive integer.

[0024] Blockchain node B_i can be any node in a blockchain network and does not particularly refer to a certain node. In practice, due to the distribution characteristic of blockchain technologies, each blockchain node in the blockchain network performs the same operation to ensure the consistency of blockchain data respectively maintained by each blockchain node. Therefore, each blockchain node can be considered as blockchain node B_i .

[0025] Based on the related technologies, a type field can be added to a blockchain transaction, so that blockchain node B_i can distinguish between different types of blockchain transactions based on a value of the type field. For example, the value of type field being 0 corresponds to a block editing transaction, and the value of type field being 1 corresponds to another blockchain transaction. Certainly, different types of blockchain transactions can be distinguished from each other in other ways. Implementations are not limited in the present specification. The block editing transaction is created by a certain transaction initiator and then sent to the blockchain network. The transaction initiator can be a certain user. Blockchain node B_i can receive the block editing transaction from a client device used by the transaction

initiator. Alternatively, the transaction initiator can send the block editing transaction to blockchain node B_j by using the client device, and blockchain node B_i can receive the block editing transaction from blockchain node B_j .

[0026] Generally, block content should be prevented from being randomly edited.

5 For example, blockchain node B_i can determine the transaction initiator of the block editing transaction, and edit the block content of block Q_i based on the block editing transaction when the transaction initiator has an editing permission for block Q_i . Otherwise, the block editing transaction may not be executed. Blockchain node B_i can manage the editing permission in various ways. For example, information about a
10 blockchain administrator can be recorded in a genesis block of the blockchain, and blockchain node B_i can consider that the transaction initiator has the editing permission only when the transaction initiator is the blockchain administrator. This way is applicable to all blocks included in the blockchain. For another example, a list of accounts having the editing permission can be included in block Q_i , and blockchain
15 node B_i can consider that the transaction initiator has the editing permission only when the transaction initiator belongs to the account list. This way is equivalent to maintaining one account list in each block, wherein account lists maintained in different blocks are independent from each other, thereby realizing block-level editing permission management with relatively higher flexibility.

20 **[0027]** Assume that the blockchain network includes n blockchain nodes, i.e. previously-mentioned blockchain nodes B_1 to B_n , and each blockchain node maintains a node public-private key pair corresponding to identity information of the blockchain node, for example, blockchain node B_1 corresponds to node public key h_1 and node private key x_1 , and blockchain node B_2 corresponds to node public key h_2
25 and node private key x_2 , ..., and blockchain node B_n corresponds to node public key h_n and node private key x_n . Blockchain node B_i needs to self-maintain node private key x_i of the blockchain node B_i and prevent node private key x_i from being leaked, and node public key h_i needs to be shared with other blockchain nodes, so that each blockchain node can know node public keys h_1 to h_n and then can generate public key
30 H based on node public keys h_1 to h_n , for generating the parent hash and performing a subsequent block editing process.

[0028] Step 204: Blockchain node B_i executes a smart contract that generates a random number when determining that a consensus on the block editing transaction succeeds, wherein the smart contract is used to execute secure multi-party computing

related to node private keys x_1 to x_n respectively corresponding to blockchain nodes B_1 to B_n to generate private key X ; and determine corresponding target random number r' based on original block content m , target block content m' , original random number r , and private key X , wherein a hash value generated through calculation by using target block content m' , public key H , and target random number r' is the same as the parent hash.

[0029] Blockchain nodes B_1 to B_n need to perform the consensus on the block editing transaction. When the consensus on the block editing transaction succeeds, it indicates that each blockchain nodes agrees to edit the block content of block Q_i based on the block editing transaction, and then the blockchain nodes execute the block editing transaction to edit the block content of block Q_i . Blockchain nodes B_1 to B_n can perform the consensus by using any type of consensus algorithm. Implementations are not limited in the present specification.

[0030] In a blockchain network using consensus algorithms such as proof of work (POW), proof of stake (POS), or delegated proof of stake (DPOS), a consensus process includes a competition for a bookkeeping right among blockchain nodes. Ethereum is taken as an example. Nodes in Ethereum are also generally nodes competing for the bookkeeping right. The blockchain nodes can perform the block editing transaction locally as nodes competing for the bookkeeping right. A certain node in all the nodes competing for the bookkeeping right becomes a bookkeeping node when winning in the current round of competition for the bookkeeping right. Assume that the blockchain node becomes the bookkeeping node when winning in the current round of competition for the bookkeeping right. Certainly, if the blockchain node does not win in the current round of competition for the bookkeeping right, the blockchain node is not the bookkeeping node, and another node may become the bookkeeping node. With regard to the blockchain network competing for the bookkeeping right, after the blockchain node in the present specification performs verification on the received block editing transaction before the consensus, if the verification succeeds, the blockchain node broadcasts the block editing transaction to the other blockchain nodes in the blockchain network, so that no matter which node is the bookkeeping node in the current round, the bookkeeping node can package the block editing transaction (or further package other transactions together) and generate a new block, and send the new block to non-bookkeeping nodes for the consensus, the non-bookkeeping nodes can add the new block to the end of the original blockchain

when verification performed by the non-bookkeeping nodes on the received new block succeeds, thereby completing the bookkeeping process and reaching the consensus. If the verification performed by the blockchain node in the present specification on the block editing transaction before the consensus fails, the
5 blockchain node does not broadcast the block editing transaction to the other blockchain nodes.

[0031] In a blockchain network using a mechanism such as practical byzantine fault tolerance (PBFT), a node having a bookkeeping right is determined through negotiation before the current round of bookkeeping. Therefore, after the blockchain
10 node receives the block editing transaction, assume that verification on the block editing transaction before the consensus succeeds, the blockchain node sends the block editing transaction to the bookkeeping node when the blockchain node is not the bookkeeping node in the current round; or packages the block editing transaction (or further packages other transactions together) and generates a new block, and then
15 sends the generated new block to non-bookkeeping nodes for the consensus when the blockchain node is the bookkeeping node in the current round. In addition, after the blockchain node receives the block editing transaction, assume that verification on the block editing transaction before the consensus fails, the blockchain node does not send the block editing transaction to the bookkeeping node when the blockchain node
20 is not the bookkeeping node in the current round, and the blockchain node does not package the block editing transaction to generate a new block when the blockchain node is the bookkeeping node in the current round. For the new block generated by the bookkeeping node, the non-bookkeeping nodes can add the new block to the end of the original blockchain after verification performed by the non-bookkeeping nodes
25 on the received new block succeeds, thereby completing the bookkeeping process and reaching the consensus.

[0032] In the related technologies, a commonly used hash algorithm $f()$ has only one input. For example, if the hash value of block Q_i is calculated, an input is the block content m of block Q_i , i.e. the hash value is $f(m)$. If block content m needs to be
30 changed to block content m' , it is necessary to just make a hash collision between m and m' to allow $f(m)=f(m')$, and such a probability is almost negligible. Therefore, the block content m actually cannot be modified as needed. However, in the technical solutions of the present specification, a used hash algorithm $f()$ has two inputs. For example, if the hash value of block Q_i is calculated, inputs are block content m and

random number r of block Q_i , i.e. the hash value is $f(m, r)$. If block content m needs to be changed to block content m' , calculated hash value $f(m, r) = f(m', r')$ can be ensured only by identifying random number r' matching block content m' . Therefore, block content m can be modified to any block content m' as needed.

5 **[0033]** Blockchain node B_i cannot randomly generate random number r' , and must use private key X corresponding to public key H . Otherwise, blockchain node B_i may randomly modify the block content. Therefore, in the present specification, a distributed private key management method is used, so that each blockchain node B_i holds only node private key x_i , and the generation of private key X is related to all
10 node private keys x_1 to x_n . In this case, any blockchain node can be prevented from obtaining private key X provided that each blockchain node maintains a node private key hold by that blockchain node and a certain blockchain node is prevented from holding all the node private keys. The present specification further provides a method for implementing secure multi-party computing by using the smart contract to
15 generate private key X and then generate random number r' based on private key X , thereby satisfying the node content editing needs while preventing the node private key or private key X from being exposed.

[0034] A smart contract can be deployed and invoked for any one of a public blockchain, a private blockchain, and a consortium blockchain. Ethereum is taken as
20 an example. Users are supported in creating and/or invoking some complex logic in an Ethereum network. It is the biggest challenge for distinguishing Ethereum from bitcoin blockchain technologies. The core of Ethereum serving as a programmable blockchain is an Ethereum virtual machine (EVM), and each Ethereum node can run an EVM. The EVM is a Turing-complete virtual machine. It means that various types
25 of complex logic can be implemented by using the EVM. Users publish and invoke smart contracts on the EVM.

[0035] For example, as shown in FIG. 3, after Bob sends a transaction including information about creating a smart contract to an Ethereum network, an EVM of node
30 1 can execute the transaction and generate a corresponding contract instance. A data field of the transaction can save code (for example, bytecode) of the smart contract, and a to field of the transaction is an empty account. After nodes reach a consensus by using a consensus mechanism, the contract is successfully created and subsequently a user can invoke the contract. After the contract is created, a contract account corresponding to the smart contract appears on the blockchain and has a specific

address. The contract code and account storage are saved in the contract account. Behavior of the smart contract is controlled by using the contract code, and the account storage of the smart contract saves a state of the contract. In other words, the smart contract enables a virtual account including the contract code and the account storage to be generated on the blockchain.

[0036] Further, as shown in FIG. 4, Ethereum is still taken as an example. Bob sends a transaction for invoking a smart contract to an Ethereum network, an EVM of node 1 can execute the transaction and generate a corresponding contract instance. In FIG. 4, a from field of the transaction is an address of an account initiating invocation of the smart contract, "0x692a70d2..." in a to field represents an address of the invoked smart contract, a value field is a value of ETH in Ethereum, and a data field of the transaction saves a method and parameters for invoking the smart contract. The smart contract can be executed independently at each node in the blockchain network in a prescribed way, and all execution records and data are saved on the blockchain. Therefore, when such a transaction is completed, a transaction certificate that cannot be tampered with or lost is saved on the blockchain.

[0037] Contract code included in the smart contract is pre-defined and checkable, and the corresponding contract code can be automatically executed after the smart contract is invoked, to implement a predefined logical function, which can ensure that the smart contract always can independently and faithfully accomplish a calculation task. Therefore, in applying the smart contract to a block editing process, the smart contract can implement calculation of private key X and random number r' without leaking private key X or data used to calculate private key X to the blockchain node, and the whole calculation process is equivalent to a "black box" for the blockchain node, thereby preventing the blockchain node from holding private key X or the data used to calculate private key X .

[0038] Private keys x_1 to x_n and derived data thereof can be shared among blockchain nodes B_1 to B_n by using a secret sharing algorithm, and shared data obtained by each blockchain node is the data used to calculate private key X . For example, blockchain node B_i can fragment node private key x_i maintained by the blockchain node B_i by using the secret sharing algorithm, to obtain private key fragments x_{i_1} to x_{i_n} . For example, blockchain node B_1 processes node private key x_1 into private key fragments x_{1_1} to x_{1_n} , blockchain node B_2 processes node private key x_2 into private key fragments x_{2_1} to x_{2_n} , ..., and blockchain node B_n

processes node private key x_n into private key fragments x_{n_1} to x_{n_n} . Then, blockchain node B_i can share private key fragment x_{i_j} with blockchain node B_j , where $j \in [1, i-1] \cup [i+1, n]$ and j is a positive integer. For example, when $i=1$, blockchain node B_1 shares private key fragment x_{1_2} with blockchain node B_2 ,
5 shares private key fragment x_{1_3} with blockchain node B_3 , ..., and shares private key fragment x_{1_n} with blockchain node B_n . For another example, when $i=2$, blockchain node B_2 shares private key fragment x_{2_1} with blockchain node B_1 , shares private key fragment x_{2_3} with blockchain node B_3 , ..., and shares private key fragment x_{2_n} with blockchain node B_n , so that blockchain node B_i can finally obtain private
10 key fragment x_{i_i} generated by the blockchain node B_i and private key fragments x_{j_i} respectively shared by other blockchain nodes B_j . It is equivalent that blockchain node B_i can finally obtain private key fragments x_{1_i} to x_{n_i} . For example, blockchain node B_1 obtains private key fragments x_{1_1} to x_{n_1} , blockchain node B_2 obtains private key fragments x_{1_2} to x_{n_2} , ..., and blockchain node B_n obtains private key
15 fragments x_{1_n} to x_{n_n} .

[0039] In this case, when the block content of block Q_i needs to be edited, each blockchain node needs to share private key fragments obtained by the blockchain node, to recover private key X . For example, blockchain node B_i can recover private key fragments x_{1_i} to x_{n_i} maintained by blockchain node B_i by using the secret
20 sharing algorithm, to obtain intermediate fragment x_i' . Then, each blockchain node can share an intermediate fragment generated by the blockchain node, so that each blockchain node can obtain intermediate fragments x_1' to x_n' . In this case, when invoking the smart contract, blockchain node B_i can use intermediate fragments x_1' to x_n' as input parameters of the smart contract, so that the smart contract can recover
25 intermediate fragments x_1' to x_n' by using the secret sharing algorithm, to obtain private key X and then generate random number r' .

[0040] In a process of invoking and executing the smart contract, blockchain node B_i may need to cache intermediate fragments x_1' to x_n' and private key X generated in the process. To prevent an untrusted application on blockchain node B_i from reading
30 intermediate fragments x_1' to x_n' or private key X from a cache, a trusted execution environment (TEE) can be deployed on blockchain node B_i , and execution of the smart contract in the TEE can be ensured.

[0041] The TEE is a security extension based on CPU hardware and is completely isolated from the outside. The TEE was originally proposed by the Global Platform to

implement secure isolation between resources on mobile devices, and is parallel to an operating system to provide a trusted secure execution environment for an application. The trust zone technology of ARM was the first to implement the real commercial TEE technology. With the rapid development of the Internet, the demand for security

5 is increasingly high, in addition to mobile devices, cloud devices and data centers propose more demands for the TEE. The concept of TEE has also been rapidly developed and expanded. The TEE now has a much broader concept than the originally proposed concept. For example, server chip vendors such as Intel and AMD have introduced hardware-assisted TEEs and enriched the concept and characteristics

10 of the TEE, which have been widely recognized in industry. The TEE now commonly refers to such a hardware-assisted TEE technology in more cases. Unlike a mobile terminal, cloud access requires remote access and users of end-user devices are invisible to a hardware platform. Therefore, the first step in using the TEE is to confirm authenticity of the TEE. Therefore, all TEE technologies now introduce a

15 remote attestation mechanism endorsed by a hardware vendor (mainly by a CPU vendor), and it is ensured that users can verify a TEE state by using digital signature technologies. However, even the secure resource isolation cannot satisfy security demands, and further data privacy protection is also proposed. Commercial TEEs, including Intel SGX and AMD SEV, also provide a memory encryption technology to

20 confine trusted hardware inside a CPU, where bus and memory data are ciphertext to prevent malicious users from snooping. For example, TEE technologies such as Intel Software Guard Extension (SGX) isolate code execution, remote attestation, security configuration, secure data storage, and trusted paths for code execution. Applications running in the TEE are secured and hardly accessible to third parties.

25 **[0042]** The Intel SGX technology is taken as an example. SGX provides an enclave, namely, an encrypted trusted execution area in a memory, where data is protected by the CPU from being stolen. For example, a first blockchain node uses a CPU supporting SGX. A partial area, an enclave page cache (EPC), can be allocated in the memory by using a newly added processor instruction, and data in the EPC is

30 encrypted by using a memory encryption engine (MEE) in the CPU. The encrypted content in the EPC is decrypted into plaintext only after entering the CPU. Therefore, in SGX, users can distrust an operating system, a virtual machine monitor (VMM), and even a basic input output system (BIOS), and only need to trust the CPU to ensure that private data is not leaked. In practice, the private data can be encrypted and

transferred to the enclave in the form of ciphertext, and a corresponding key can also be transferred to the enclave through remote attestation. Then, the data is used for calculation under encryption protection of the CPU, and a result is returned in the form of ciphertext. In this mode, strong computing power can be used without
5 concern for data leakage.

[0043] The smart contract can further actively delete generated private key X , for example, clear cache space for storing private key X , after determining target random number r' . Similarly, the smart contract can actively delete intermediate fragments $x1'$ to xn' , for example, clear cache space for storing intermediate fragments $x1'$ to xn' ,
10 after determining private key X . The cache space is actively cleared, so that an untrusted application can be prevented from stealing private key X or intermediate fragments $x1'$ to xn' from the cache, thereby improving security.

[0044] The related technologies include many hash algorithms that satisfy the operation demands of the present specification, such as a chameleon hash algorithm.

15 Taking the chameleon hash algorithm as an example, a hash value calculation formula is: $HASH = g^a * H^b$, where g is a predetermined generator, H is a public key, a is data, and b is a random number. For example, when a is block content m , b is random number r ; or when a is block content m' , b is random number r' . Therefore, parent hash $HASH_Qi = g^m * H^r$ can be calculated.

20 **[0045]** Because the node public-private key pair satisfies $hi = g^{xi}$, public key $H = h1 * h2 * \dots * hn$ and private key $X = x1 + x2 + \dots + xn$ are set, and then the parent hash is obtained as follows:

$HASH_Qi = g^m * H^r = g^m * (h1 * h2 * \dots * hn)^r = g^m * (g^{x1} * g^{x2} * \dots * g^{xn})^r = g^{[m + (x1 + x2 + \dots + xn) * r]} = g^{(m + Xr)}$. Similarly, a corresponding parent hash obtained after

25 block editing can be calculated as follows:

$HASH_Qi' = g^{m'} * H^{r'} = g^{m'} * (h1 * h2 * \dots * hn)^{r'} = g^{m'} * (g^{x1} * g^{x2} * \dots * g^{xn})^{r'} = g^{[m' + (x1 + x2 + \dots + xn) * r']} = g^{(m' + Xr')}$. Because the parent hash values obtained before and after the block editing need to be consistent, namely, $HASH_Qi = HASH_Qi'$, $g^{(m + Xr)} = g^{(m' + Xr')}$ can be obtained, and then random number $r' = (m + Xr - m') / X$ can

30 be determined.

[0046] It can be seen that private key X can be calculated by using the smart contract, and random number r' can be calculated by using private key X , random number r , block content m , and block content m' . In addition, because values of random number r , block content m , and block content m' are all known, private key X is the central

factor for successfully calculating random number r' . Therefore, private key X and the data used to calculate private key X need to be encrypted in the previously described way. Otherwise, the block content can be randomly modified based on private key X and the data used to calculate private key X , resulting in a security risk.

5 [0047] Step 206: Blockchain node B_i updates original block content m to target block content m' and original random number r to target random number r' .

[0048] Blockchain node B_i needs to add the hash value of block Q_i , namely, parent hash $HASH_Q_i$, to the block header of the block Q_{i+1} when generating block Q_{i+1} . Because the calculation of parent hash $HASH_Q_i$ relates to block content m , random
10 number r , and public key H , and both block content m and random number r are fixed, the value of parent hash $HASH_Q_i$ is affected by public key H . The public key H is calculated by using node public keys h_1 to h_n corresponding to the blockchain nodes. Therefore, in the process of generating block Q_{i+1} , blockchain node B_i needs to determine node public key h_i used for block Q_i , send determined node public key h_i
15 to the other blockchain nodes, and receive node public keys used for block Q_i that are determined by the other blockchain nodes, so that each blockchain node finally obtains node public key h_1 to h_n , to generate public key H and then generate parent hash $HASH_Q_i$.

[0049] If the node public-private key pair used by each blockchain node keeps
20 unchanged, i.e. blockchain node B_i always uses public-private key pair (h_i, x_i) , the value of public key H also keeps unchanged, so that the blockchain node needs to share the node public key only once, instead of sharing the node public key when each block is generated. However, long-term invariance of the public-private key pair may lead to a security risk. Therefore, the blockchain node can periodically or temporarily
25 change the used public-private key pair. As such, even if some public-private key pairs are leaked, not all blocks are at risk of being tampered with. If a periodical change method is used, all the blockchain nodes change the public-private key pairs used by the blockchain nodes based on a fixed period, and the blockchain nodes can share the changed node public key in the process of generating the first block after
30 each change, but do not need to share the changed node public key in the rest of the same period. If a temporary change method is used, each blockchain node cannot determine whether the other blockchain nodes are to change their public-private key pairs. Therefore, it is necessary to share the node public key each time a block is

generated. The temporary change method is more random than the periodic change method, thereby achieving higher security.

[0050] As previously described, if the node public-private key pair used by each blockchain node is unchanged, blockchain node Bi inevitably uses the same public-private key pair for different blocks, so that the number of sharing times of the node public key can be minimized. However, if the blockchain node changes the public-private key pair, blockchain node Bi uses different public-private key pairs for at least two blocks. So that blockchain node Bi needs to record a mapping relationship between each block and a correspondingly used public-private key pair. As such, in the subsequent editing for the block content of block Qi , the block content of block Qi can be edited based on the mapping relationship. For example, it can be ensured that blockchain node Bi uses a correct private key fragment to generate a corresponding intermediate fragment, and then correct private key X is ensured.

[0051] FIG. 5 is a schematic structural diagram illustrating a device according to an example embodiment. Referring to FIG. 5, at a hardware level, the device includes a processor 502, an internal bus 504, a network interface 506, a memory 508, and a non-volatile memory 510. Certainly, the device may further include hardware needed by other services. The processor 502 reads a corresponding computer program from the non-volatile memory 510 to the memory 508 and then runs the computer program to form a block content editing apparatus at a logical level. Certainly, in addition to a software implementation, the one or more embodiments of the present specification do not exclude other implementations, such as a logic device or a combination of hardware and software, i.e. an execution body of the following processing procedure is not limited to each logic unit, and can be a hardware or logic device.

[0052] Referring to FIG. 6, in the software implementation, the block content editing apparatus can include:

[0053] a receiving unit 61, configured to enable blockchain node Bi to receive a block editing transaction, which is used to edit original block content m of block Qi to target block content m' , where a parent hash corresponding to block Qi is recorded in a block header of block $Qi+1$, the parent hash is generated through calculation by using original block content m , public key H , and original random number r , public key H is generated through calculation by using node public keys $h1$ to hn respectively corresponding to blockchain nodes $B1$ to Bn , and $i \in [1, n]$ and i is a positive integer

- [0054] an execution unit 62, configured to enable blockchain node Bi to execute a smart contract that generates a random number when determining that a consensus on the block editing transaction succeeds, where the smart contract is used to execute secure multi-party computing related to node private keys $x1$ to xn respectively
- 5 corresponding to blockchain nodes $B1$ to Bn to generate private key X ; and determine corresponding target random number r' based on original block content m , target block content m' , original random number r , and private key X , where a hash value generated through calculation by using target block content m' , public key H , and target random number r' is the same as the parent hash; and
- 10 [0055] an updating unit 63, configured to enable blockchain node Bi to update original block content m to target block content m' and original random number r to target random number r' .
- [0056] Optionally, the execution unit 62 generates private key X through secure multi-party computing, including the following:
- 15 [0057] obtaining intermediate fragments $x1'$ to xn' , where intermediate fragment xi' is obtained by blockchain node Bi by recovering private key fragments $x1_i$ to xn_i by using a secret sharing algorithm, private key fragments xi_1 to xi_n are obtained by blockchain node Bi by fragmenting node private key xi by using the secret sharing algorithm, xi_j is shared with by blockchain node Bi blockchain node Bj , and $j \in [1,$
- 20 $i-1] \cup [i+1, n]$ and j is a positive integer; and
- [0058] recovering intermediate fragments $x1'$ to xn' by using the secret sharing algorithm, to obtain private key X .
- [0059] Optionally, the execution unit 62 is specifically configured to:
- [0060] execute the smart contract that generates the random number in a trusted
- 25 execution environment deployed on blockchain node Bi .
- [0061] Optionally, the smart contract is further used to delete generated private key X when target random number r' is determined.
- [0062] Optionally, public key H is a product of node public keys $h1$ to hn , private key X is a sum of node private keys $x1$ to xn , and $hi = g^{xi}$ when a hash value is
- 30 calculated by using a formula g^{a*H^b} , where
- [0063] g is a predetermined generator; and $a=m$ and $b=r$, or $a=m'$ and $b=r'$.
- [0064] Optionally, the block content editing apparatus further includes:

[0065] an initiator determining unit 64, configured to enable blockchain node Bi to determine a transaction initiator of the block editing transaction; and

[0066] the updating unit 63 is configured to enable blockchain node Bi to update the block content of block Qi based on the block editing transaction when the transaction initiator has an editing permission for block Qi .

[0067] Optionally, the block content editing apparatus further includes:

[0068] a public key determining unit 65, configured to enable blockchain node Bi to determine node public key hi used for block Qi in a process of generating block $Qi+1$;

[0069] a sending unit 66, configured to enable blockchain node Bi to send determined node public key hi to the other blockchain nodes, and receive node public keys used for block Qi that are determined by the other blockchain nodes, to obtain node public keys $h1$ to hn ; and

[0070] a generation unit 67, configured to enable blockchain node Bi to generate the parent hash based on public key H corresponding to node public keys $h1$ to hn , and add the parent hash to the block header of block $Qi+1$.

[0071] Optionally, blockchain node Bi uses the same public-private key pair for different blocks; or

[0072] when blockchain node Bi uses different public-private key pairs for at least two blocks, the apparatus further includes: a recording unit 68, configured to enable blockchain node Bi to record a mapping relationship between each block and a correspondingly used public-private key pair to edit the block content of block Qi based on the mapping relationship..

[0073] The systems, methods, modules, or units illustrated in the previous embodiments can be implemented by using a computer chip or an entity, or can be implemented by using a product having a certain function. A typical implementation device is a computer. A specific form of the computer can be a personal computer, a laptop computer, a cellular phone, a camera phone, a smartphone, a personal digital assistant, a media player, a navigation device, an email sending/receiving device, a game console, a tablet computer, a wearable device, or a combination of any several of these devices.

[0074] In a typical configuration, the computer includes one or more processors (CPUs), input/output interfaces, network interfaces, and memories.

[0075] The memory may include forms such as a non-persistent memory, a random access memory (RAM), and/or a non-volatile memory in a computer-readable

medium, such as a read-only memory (ROM) or a flash memory (flash RAM). The memory is an example of the computer-readable medium.

[0076] The computer-readable medium includes persistent, non-persistent, movable, and unmovable media that can store information by using any method or technology.

5 The information can be a computer-readable instruction, a data structure, a program module, or other data. Examples of the computer storage medium include but are not limited to a phase-change random access memory (PRAM), a static random access memory (SRAM), a dynamic random access memory (DRAM), a random access memory (RAM) of another type, a read-only memory (ROM), an electrically erasable
10 programmable ROM (EEPROM), a flash memory or another memory technology, a compact disc read-only memory (CD-ROM), a digital versatile disc (DVD) or another optical storage, a cassette, a magnetic disk storage, a quantum memory, a graphene-based storage medium or another magnetic storage device, or any other non-transmission medium. The computer storage medium can be configured to store
15 information accessible to a computing device. As described in the present specification, the computer-readable medium does not include computer-readable transitory media such as a modulated data signal and a carrier.

[0077] It is worthwhile to note that the terms "comprise", "include", or any other variation thereof are intended to cover a non-exclusive inclusion, so that a process,
20 method, product, or device that includes a list of elements includes those elements and further includes other elements not expressly listed or inherent to such a process, method, product, or device. An element preceded by the phrase "comprise a..." does not, without more constraints, preclude the existence of additional identical elements in a process, method, product, or device that includes the element.

25 **[0078]** The specific embodiments of the present specification are previously described. Other embodiments fall within the scope of the appended claims. In some cases, the actions or steps in the claims can be performed in different orders from the orders in the embodiments and still can achieve the desired results. In addition, the processes illustrated in the accompanying drawings do not necessarily require the
30 shown specific order or sequence to achieve the desired results. In some implementations, multitasking and parallel processing are also possible or may be advantageous.

[0079] The terms used in the one or more embodiments of the present specification are intended merely for the purpose of describing specific embodiments and are not

intended to limit the one or more embodiments of the present specification. As used in the one or more embodiments of the present specification and the claims, singular forms "a", "an" and "the" are also intended to include plural forms, unless otherwise specified in the context clearly. It should also be understood that the term "and/or" used in the present specification refers to and includes any or all possible combinations of one or more associated listed items.

[0080] It should be understood that, although terms "first", "second", "third", etc. may be used in describing various types of information in the one or more embodiments of the present specification, such information should not be limited to such terms. These terms are only used to distinguish between information of the same type. For example, first information can also be referred to as second information, and similarly, second information can also be referred to as first information, without departing from the scope of the one or more embodiments of the present specification. Depending on the context, the word "if" used here can be interpreted as "at the time of", "when" or "in response to determining".

[0081] The previous descriptions are merely preferred embodiments of the one or more embodiments of the present specification, and are not intended to limit the one or more embodiments of the present specification. Any modification, equivalent substitution, improvement, etc. made within the spirit and principles of the one or more embodiments of the present specification shall fall within the protection scope of the one or more embodiments of the present specification.

CLAIMS

What is claimed is:

1. A block content editing method, comprising:

receiving, by a blockchain node Bi , a block editing transaction, which is used to
5 edit original block content m of a block Qi to target block content m' , wherein a parent
hash corresponding to the block Qi is recorded in a block header of a block $Qi+1$, the
parent hash is generated through calculation by using original block content m , a public
key H , and an original random number r , the public key H is generated through
calculation using node public keys $h1$ to hn respectively corresponding to blockchain
10 nodes $B1$ to Bn , and $i \in [1, n]$ and i is a positive integer;

executing, by the blockchain node Bi , a smart contract that generates a random
number when determining that a consensus on the block editing transaction succeeds,
wherein the smart contract is used to execute secure multi-party computing related to
node private keys $x1$ to xn respectively corresponding to the blockchain nodes $B1$ to Bn
15 to generate a private key X ; and determining corresponding target random number r'
based on the original block content m , the target block content m' , the original random
number r , and the private key X , wherein a hash value generated through calculation by
using the target block content m' , the public key H , and the target random number r' is
the same as the parent hash; and

20 updating, by the blockchain node Bi , the original block content m to the target
block content m' and the original random number r to the target random number r' ,
wherein generating the private key X through the secure multi-party computing
comprises:

obtaining intermediate fragments $x1'$ to xn' , wherein an intermediate fragment
25 xi' is obtained by the blockchain node Bi via recovering private key fragments xi_1 to
 xn_i using a secret sharing algorithm, the private key fragments xi_1 to xi_n are
obtained by the blockchain node Bi via fragmenting a node private key xi using the
secret sharing algorithm, xi_j is shared by the blockchain node Bi with a blockchain
node Bj , and $j \in [1, i-1] \cup [i+1, n]$ and j is a positive integer; and

30 obtaining the private key X by recovering the intermediate fragments $x1'$ to
 xn' using the secret sharing algorithm.

2. The method according to claim 1, wherein the executing a smart contract that generates a random number comprises:

executing the smart contract that generates the random number in a trusted execution environment deployed on the blockchain node Bi .

5 3. The method according to claim 1, wherein the smart contract is further used to delete the generated private key X when the target random number r' is determined.

4. The method according to claim 1, wherein the public key H is a product of the node public keys $h1$ to hn , the private key X is a sum of the node private keys $x1$ to xn , and $hi=g^{xi}$ when the hash value is calculated by using a formula $g^a \cdot H^b$, wherein

10 g is a predetermined generator; and $a=m$ and $b=r$, or $a=m'$ and $b=r'$.

5. The method according to claim 1, further comprising:

determining, by the blockchain node Bi , a transaction initiator of the block editing transaction; and

15 updating, by the blockchain node Bi , block content of the block Qi based on the block editing transaction when the transaction initiator has an editing permission for the block Qi .

6. The method according to claim 1, further comprising:

determining, by the blockchain node Bi , a node public key hi used for the block Qi in a process of generating the block $Qi+1$;

20 sending, by the blockchain node Bi , the determined node public key hi to the other blockchain nodes, and receiving node public keys used for the block Qi that are determined by the other blockchain nodes, to obtain the node public keys $h1$ to hn ; and

generating, by the blockchain node Bi , the parent hash based on the public key H corresponding to the node public keys $h1$ to hn , and adding the parent hash to the block

25 header of block $Qi+1$.

7. The method according to claim 1, wherein

the blockchain node Bi uses a same public-private key pair for different blocks; or

when the blockchain node Bi uses different public-private key pairs for at least two blocks, the method further comprises: recording, by the blockchain node Bi , a mapping relationship between each block and a correspondingly used public-private key pair to edit the block content of the block Qi based on the mapping relationship.

30

8. A block content editing apparatus, comprising:

a receiving unit, configured to enable a blockchain node B_i to receive a block editing transaction, which is used to edit original block content m of a block Q_i to target block content m' , wherein a parent hash corresponding to the block Q_i is recorded in a block header of a block Q_{i+1} , the parent hash is generated through calculation by using
5 the original block content m , a public key H , and an original random number r , the public key H is generated through calculation using node public keys h_1 to h_n respectively corresponding to blockchain nodes B_1 to B_n , and $i \in [1, n]$ and i is a positive integer;

an execution unit, configured to enable the blockchain node B_i to execute a smart
10 contract that generates a random number when determining that a consensus on the block editing transaction succeeds, wherein the smart contract is used to execute secure multi-party computing related to node private keys x_1 to x_n respectively corresponding to the blockchain nodes B_1 to B_n to generate a private key X ; and determine corresponding target random number r' based on the original block content m , the target
15 block content m' , the original random number r , and the private key X , wherein a hash value generated through calculation by using the target block content m' , the public key H , and the target random number r' is the same as the parent hash; and

an updating unit, configured to enable the blockchain node B_i to update the original block content m to the target block content m' and the original random number r to the
20 target random number r' , wherein generating the private key X through the secure multi-party computing comprises:

obtaining intermediate fragments x_1' to x_n' , wherein an intermediate fragment x_i' is obtained by the blockchain node B_i via recovering private key fragments x_{1_i} to x_{n_i} using a secret sharing algorithm, the private key fragments x_{1_i} to x_{n_i} are
25 obtained by the blockchain node B_i via fragmenting a node private key x_i using the secret sharing algorithm, x_{i_j} is shared by the blockchain node B_i with a blockchain node B_j , and $j \in [1, i-1] \cup [i+1, n]$ and j is a positive integer; and

obtaining the private key X by recovering the intermediate fragments x_1' to x_n' using the secret sharing algorithm.

30 9. A blockchain node, comprising:

a processor; and

a memory configured to store a processor-executable instruction, wherein

the processor implements the method according to any one of claims 1 to 7 by executing the executable instruction.

10. A computer-readable storage medium, storing a computer instruction, wherein the step of the method according to any one of claims 1 to 7 is implemented when the
- 5 instruction is executed by a processor.