

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' ;

~~2. The method according to claim 1~~, 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.

32. 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 43. 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.

54. 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*H^b} , wherein

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

65. 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 .

76. 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 ~~a-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 header of block $Qi+1$.

87. 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

98. 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 to x_n using a secret sharing algorithm, the private key fragments x_1 to x_n are
25 obtained by the blockchain node B_i via fragmenting a node private key x_i using the secret sharing algorithm, x_i 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 ~~409~~. 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 ~~8~~7 by executing the executable instruction.

~~41~~10. A computer-readable storage medium, storing a computer instruction, wherein the step of the method according to any one of claims 1 to ~~8~~7 is implemented
5 when the instruction is executed by a processor.