

CLAIMS

1. A computer-implemented method, comprising:

for each transaction storage location in a target block of a blockchain network that
5 comprises a full node and a light node, retrieving, by the full node in the blockchain network, data
from a respective transaction storage location;

analyzing the data retrieved from the each transaction storage location;

determining, for each transaction storage location, whether the data retrieved from the
respective transaction storage location is transaction or concealed data;

10 in response to determining that the data retrieved is transaction, performing a hash
operation on the transaction to obtain a transaction hash;

in response to determining that the data retrieved is concealed data, extracting the
transaction hash from the concealed data, wherein the transaction hash is a hash value of the
transaction stored at the transaction storage location, and each node in the blockchain network
15 is instructed by a node that has permission to perform transaction concealment to replace the
transaction stored at the transaction storage location with the concealed data, comprising:

obtaining the transaction hash of the transaction stored at the transaction storage
location; and

concatenating one or more front marking characters indicating that the data
20 retrieved is concealed data and rather than transaction to a header of the transaction hash to
generate a first concatenation, wherein the header is at a front of the transaction hash;

generating the Merkle tree corresponding to the target block based on transaction
hashes that correspond to the transaction storage locations in the target block; and

in response to receiving a verification request of a target transaction:

25 determining, from the Merkle tree that has been generated based on the transaction
or the concealed data or both, a Merkle tree path to the target transaction;

computing a hash value associated with the Merkle tree path to the target
transaction; and

providing the hash value associated with the Merkle tree path to the target
30 transaction that has been computed from the Merkle tree generated based on the transaction or
the concealed data or both to the light node for use in a simplified payment verification (SPV)
of the target transaction.

2. The computer-implemented method according to claim 1, wherein replacing the transaction stored at the transaction storage location with the concealed data comprises:

identifying the concealed data based on the first concatenation; and

replacing the transaction stored at the transaction storage location with the concealed data.

3. The computer-implemented method according to claim 2, wherein identifying the concealed data based on the first concatenation comprising:

concatenating a predetermined rear marking character to an end of the first concatenation;

concatenating a remark to an end of the predetermined rear marking character to generate a second concatenation, wherein the predetermined rear marking character separates the transaction hash and the remark; and

identifying the second concatenation as the concealed data.

4. The computer-implemented method according to claim 2, wherein analyzing the data retrieved from the transaction storage location comprises:

determining whether the data retrieved from the transaction storage location comprises the front marking character;

in response to determining that the data retrieved from the transaction storage location does not comprise the front marking character, identifying the data retrieved from the transaction storage location as the transaction; and

in response to determining that the data retrieved from the transaction storage location comprises the front marking character, identifying the data retrieved from the transaction storage location as the concealed data.

5. The computer-implemented method according to claim 2, wherein extracting the transaction hash from the concealed data comprises:

identifying information located after the front marking character in the concealed data as the transaction hash; and

extracting the transaction hash.

6. The computer-implemented method according to claim 3, wherein extracting the transaction hash from the concealed data comprises:

identifying information located between the front marking character and the rear marking character in the concealed data as the transaction hash; and

5 extracting the transaction hash, wherein the transaction hash comprises a hash value obtained from performing a hash operation on a corresponding transaction only.

7. The computer-implemented method of claim 1, further comprising:

10 receiving, by the full node, the verification request, wherein the verification request comprises a target transaction identifier of the target transaction;

identifying, in the blockchain associated with the full node based on the verification request, the block in which the target transaction corresponding to the target transaction identifier is located; and

15 triggering the simplified payment verification (SPV) procedure for the target transaction corresponding to the target transaction identifier based on the Merkle tree path to the target transaction.

8. The computer-implemented method according to claim 7, wherein a correspondence between a transaction identifier of the transaction and the transaction storage
20 location of the transaction in the blockchain is pre-stored in the each node of the blockchain network, and wherein identifying the block in which the transaction corresponding to the target transaction identifier is located comprises:

identifying the transaction storage location corresponding to the target transaction identifier as a target transaction storage location based on the correspondence; and

25 identifying the block that comprises the target transaction storage location as the block in which the transaction is located.

9. A non-transitory, computer-readable medium storing one or more instructions executable by a computer system to perform operations comprising:

30 for each transaction storage location in a target block of a blockchain network that comprises a full node and a light node, retrieving, by the full node in the blockchain network, data from a respective transaction storage location;

analyzing the data retrieved from the each transaction storage location;

determining, for each transaction storage location, whether the data retrieved from the respective transaction storage location is transaction or concealed data;

5 in response to determining that the data retrieved is transaction, performing a hash operation on the transaction to obtain a transaction hash;

10 in response to determining that the data retrieved is concealed data, extracting the transaction hash from the concealed data, wherein the transaction hash is a hash value of the transaction stored at the transaction storage location, and each node in the blockchain network is instructed by a node that has permission to perform transaction concealment to replace the transaction stored at the transaction storage location with the concealed data, comprising:

obtaining the transaction hash of the transaction stored at the transaction storage location; and

15 concatenating one or more front marking characters indicating that the data retrieved is concealed data and rather than transaction to a header of the transaction hash to generate a first concatenation, wherein the header is at a front of the transaction hash;

generating the Merkle tree corresponding to the target block based on transaction hashes that correspond to the transaction storage locations in the target block; and

in response to receiving a verification request of a target transaction:

20 determining, from the Merkle tree that has been generated based on the transaction or the concealed data or both, a Merkle tree path to the target transactions;

computing a hash value associated with the Merkle tree path to the target transaction; and

25 providing the hash value associated with the Merkle tree path to the target transaction that has been computed from the Merkle tree generated based on the transaction or the concealed data or both to the light node for use in a simplified payment verification (SPV) of the target transaction.

30 10. The non-transitory, computer-readable medium according to claim 9, wherein replacing the transaction stored at the transaction storage location with the concealed data comprises:

identifying the concealed data based on the first concatenation; and

replacing the transaction stored at the transaction storage location with the concealed data.

11. The non-transitory, computer-readable medium according to claim 10, wherein
5 identifying the concealed data based on the first concatenation comprising:
concatenating a predetermined rear marking character to an end of the first concatenation;
concatenating a remark to an end of the predetermined rear marking character to generate
a second concatenation, wherein the predetermined rear marking character separates the
transaction hash and the remark; and
10 identifying the second concatenation as the concealed data.

12. The non-transitory, computer-readable medium according to claim 10, wherein
analyzing the data retrieved from the transaction storage location comprises:
determining whether the data retrieved from the transaction storage location comprises the
15 front marking character;
in response to determining that the data retrieved from the transaction storage location
does not comprise the front marking character, identifying the data retrieved from the transaction
storage location as the transaction; and
in response to determining that the data retrieved from the transaction storage location
20 comprises the front marking character, identifying the data retrieved from the transaction storage
location as the concealed data.

13. The non-transitory, computer-readable medium according to claim 10, wherein
extracting the transaction hash from the concealed data comprises:
25 identifying information located after the front marking character in the concealed data as
the transaction hash; and
extracting the transaction hash, wherein the transaction hash comprises a hash value
obtained from performing a hash operation on a corresponding transaction only.

14. The non-transitory, computer-readable medium according to claim 11, wherein
30 extracting the transaction hash from the concealed data comprises:

identifying information located between the front marking character and the rear marking character in the concealed data as the transaction hash; and

extracting the transaction hash, wherein the transaction hash comprises a hash value obtained from performing a hash operation on a corresponding transaction only.

5

15. The non-transitory, computer-readable medium of claim 9, the operations further comprising:

receiving, by the full node, the verification request, wherein the verification request comprises a target transaction identifier of the target transaction;

10 identifying, in the blockchain associated with the full node based on the verification request, the block in which the target transaction corresponding to the target transaction identifier is located; and

triggering the simplified payment verification (SPV) procedure for the target transaction corresponding to the target transaction identifier based on the Merkle tree path to the target transaction.

15

16. The non-transitory, computer-readable medium according to claim 15, wherein a correspondence between a transaction identifier of the transaction and the transaction storage location of the transaction in the blockchain is pre-stored in the each of the blockchain network, and wherein identifying the block in which the transaction corresponding to the target transaction identifier is located comprises:

20

identifying the transaction storage location corresponding to the target transaction identifier as a target transaction storage location based on the correspondence; and

identifying the block that comprises the target transaction storage location as the block in which the transaction is located.

25

17. A computer-implemented system, comprising:

one or more computers; and

one or more computer memory devices interoperably coupled with the one or more computers and having tangible, non-transitory, machine-readable media storing one or more instructions that, when executed by the one or more computers, perform one or more operations comprising:

30

for each transaction storage location in a target block of a blockchain network that comprises a full node and a light node, retrieving, by the full node in the blockchain network, data from a respective transaction storage location;

analyzing the data retrieved from the each transaction storage location;

5 determining, for each transaction storage location, whether the data retrieved from the respective transaction storage location is transaction or concealed data;

in response to determining that the data retrieved is transaction, performing a hash operation on the transaction to obtain a transaction hash;

10 in response to determining that the data retrieved is concealed data, extracting the transaction hash from the concealed data, wherein the transaction hash is a hash value of the transaction stored at the transaction storage location, and each node in the blockchain network is instructed by a node that has permission to perform transaction concealment to replace the transaction stored at the transaction storage location with the concealed data, comprising:

15 obtaining the transaction hash of the transaction stored at the transaction storage location; and

concatenating one or more front marking characters indicating that the data retrieved is concealed data and rather than transaction to a header of the transaction hash to generate a first concatenation, wherein the header is at a front of the transaction hash;

20 generating the Merkle tree corresponding to the target block based on transaction hashes that correspond to the transaction storage locations in the target block; and

in response to receiving a verification request of a target transaction:

determining, from the Merkle tree that has been generated based on the transaction or the concealed data or both, a Merkle tree path to the target transaction;

25 computing a hash value associated with the Merkle tree path to the target transaction; and

30 providing the hash value associated with the Merkle tree path to the target transaction that has been computed from the Merkle tree generated based on the transaction or the concealed data or both to the light node for use in a simplified payment verification (SPV) of the target transaction.

18. The computer-implemented system according to claim 17, wherein replacing the transaction stored at the transaction storage location with the concealed data comprises:

identifying the concealed data based on the first concatenation; and

replacing the transaction stored at the transaction storage location with the concealed

5 data.

19. The computer-implemented system according to claim 18, wherein identifying the concealed data based on the first concatenation comprising:

concatenating a predetermined rear marking character to an end of the first concatenation;

10 concatenating a remark to an end of the predetermined rear marking character to generate a second concatenation, wherein the predetermined rear marking character separates the transaction hash and the remark; and

identifying the second concatenation as the concealed data.

15 20. The computer-implemented system according to claim 18, wherein analyzing the data retrieved from the transaction storage location comprises:

determining whether the data retrieved from the transaction storage location comprises the front marking character;

20 in response to determining that the data retrieved from the transaction storage location does not comprise the front marking character, identifying the data retrieved from the transaction storage location as the transaction; and

in response to determining that the data retrieved from the transaction storage location comprises the front marking character, identifying the data retrieved from the transaction storage location as the concealed data.

25