

CLAIMS

~~What is claimed is:~~

1. A ~~Merkle tree construction~~computer-implemented method, comprising:
 - 5 for each transaction storage ~~position~~location in a target block, ~~reading, by a target full node, data from the transaction storage position, wherein the target full node is any full node in~~ of a blockchain network, that comprises a full node and a light node,
~~retrieving, by the target block is any block~~full node in a blockchain ~~of the target full node~~network, data from a respective transaction storage location;
 - 10 analyzing the data ~~read~~retrieved from the each transaction storage ~~position~~location;
~~if it is determined that the data read from the~~ determining, for each transaction storage ~~position is a~~ location, whether the data retrieved from the respective transaction storage location is transaction or concealed data;
 - 15 in response to determining that the data retrieved is transaction, performing a hash operation on the transaction, ~~to obtain a transaction hash; or~~
~~if it is determined in response to determining~~ that the data ~~read from the transaction storage position~~retrieved is concealed data, extracting ~~a~~the transaction hash from the concealed data, wherein the transaction hash ~~extracted from the~~
20 ~~concealed data is a transaction is a~~ hash value of ~~a~~the transaction ~~originally stored at the transaction storage position~~, and ~~an operation of replacing, with each node in the concealed data,~~ blockchain network is instructed by a node that has permission to perform transaction concealment to replace the transaction ~~originally stored at the transaction storage position is performed by a node having a transaction concealment~~
25 ~~permission in the blockchain network by instructing each node; and~~
~~constructing a Merkle tree corresponding to the target block based on transaction hashes respectively corresponding to transaction storage positions in the target block.~~
 2. The method according to claim 1, wherein the operation of replacing, location
with the concealed data, ~~the transaction stored at the transaction storage position is as~~
30 followscomprising:
 - obtaining the transaction hash of the transaction stored at the transaction storage ~~position;~~location; and

concatenating ~~a predetermined~~ one or more front marking ~~character~~ characters indicating that the data retrieved is concealed data and rather than transaction to a header of the transaction hash;

~~determining the concealed data based on data obtained by concatenating~~
5 ~~the~~ to generate a first concatenation, wherein the header is at a front marking character ~~and of~~ the transaction hash; ~~and~~

~~replacing, with the concealed data, 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~~

10 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;~~

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

15 ~~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.~~

20 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 ~~position~~ location
25 ~~with the concealed data.~~

~~3.~~

3. The computer-implemented method according to claim 2, wherein ~~the~~
~~determining~~ identifying the concealed data based on ~~data obtained by concatenating the~~
~~front marking character and the transaction hash specifically comprises the~~
30 ~~following~~ the first concatenation comprising:

concatenating a predetermined rear marking character to an end of the
~~transaction hash, and~~ first concatenation;

concatenating a remark ~~information~~ to an end of the predetermined rear marking character; ~~and~~

~~determining, as to generate a second concatenation, wherein the concealed data, data obtained by concatenating the front~~predetermined rear marking character;
5 separates the transaction hash, ~~the rear marking character,~~ and the remark ~~information;~~
and

~~4. identifying the second concatenation as the concealed data.~~

4. The computer-implemented method according to claim 2 ~~or 3~~, wherein ~~the~~
10 analyzing the data ~~read~~retrieved from the transaction storage position
specificallylocation comprises ~~the following:~~

~~if~~determining whether the data ~~read~~retrieved from the transaction storage
~~position~~location comprises the front marking character;

in response to determining that the data retrieved from the transaction storage
15 location does not comprise the front marking character, ~~determining, as the transaction,~~
~~the data read from the transaction storage position; or~~

~~if the data read~~identifying the data retrieved from the transaction storage
~~position comprises the front marking character,~~location as the transaction; and

in response to determining, as that the concealed data, the data read retrieved
20 from the transaction storage ~~position~~location
~~5. 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 ~~the~~
25 extracting ~~at the~~ transaction hash from the concealed data ~~specifically~~ comprises ~~the~~
following:

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

extracting the transaction hash.

30 ~~6.~~

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

~~determining data~~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;~~ and

7. ~~A simplified payment verification (SPV)~~extracting the transaction hash,
5 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:
receiving, by ~~a target~~the full node, ~~at the~~ verification request, wherein the
10 verification request comprises a target transaction identifier, ~~and of the target full node~~
~~is any full node~~transaction;

identifying, in at the blockchain network;
~~determining, in a blockchain of the target~~associated with the full node based on
the verification request, ~~at the~~ block ~~that in which the target~~ transaction corresponding
15 to the target transaction identifier is located ~~in, and constructing a Merkle tree~~
~~corresponding to the block based on the method according to any one of claims 1 to 6;~~
and

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

8. The computer-implemented method according to claim 7, wherein ~~for any~~
~~transaction written to the blockchain,~~ a correspondence between a transaction
identifier of the transaction and ~~at the~~ transaction storage position~~location~~ of the
transaction in the blockchain is pre-~~recorded on~~ stored in the each node ~~in the~~
25 ~~blockchain network;~~ and

~~the determining, in a blockchain of the target full node based on~~blockchain
network, and wherein identifying the target transaction identifier, a block that
in which the transaction corresponding to the target transaction identifier is
located ~~in specifically~~ comprises ~~the following:~~

30 ~~determining~~identifying the transaction storage position~~location~~ corresponding
to the target transaction identifier as a target transaction storage position~~location~~ based
on the ~~target transaction identifier and the pre-recorded~~ correspondence ~~between the~~
~~transaction identifier and the transaction storage position;~~ and

~~determining, as identifying the block that the transaction corresponding to the target transaction identifier is located in, a block that comprises comprises the target transaction storage position.~~

~~9. location as the block in which the transaction is located.~~

5

~~9. A Merkle tree construction apparatus, wherein the apparatus is any full node non-transitory, computer-readable medium storing one or more instructions executable by a computer system to perform operations comprising:~~

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

~~a reading module, configured to: analyzing the data retrieved from the each transaction storage location;~~

~~determining, for each transaction storage position in a target block, read data from the transaction storage position, wherein the target block is any block in a blockchain of the apparatus;~~

~~an analysis module, configured to analyze the data read from the transaction storage position;~~

~~a transaction hash determination module, configured to: if it is determined that location, whether the data read retrieved from the respective transaction storage position location is a transaction, perform 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; or if it is determined~~

~~in response to determining that the data read from the transaction storage position retrieved is concealed data, extract extracting the transaction hash from the concealed data, wherein the transaction hash extracted from the concealed data is a transaction hash value of a transaction originally stored at the transaction storage position; an operation of replacing, with the concealed data, the transaction originally the transaction stored at the transaction storage position location, and each node in the blockchain network is performed instructed by a node having that has permission to perform transaction concealment permission in the blockchain network by instructing each node; and to replace the transaction stored at the transaction storage location with the concealed data, comprising:~~

~~a Merkle tree construction module, configured to construct a Merkle tree corresponding to the target block based on transaction hashes respectively corresponding to transaction storage positions in the target block.~~

10. ~~The apparatus according to claim 9, wherein the operation of replacing, with the concealed data, the transaction stored at the transaction storage position is as follows:~~

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

~~concatenating a predetermined one or more front marking character characters indicating that the data retrieved is concealed data and rather than transaction to a header of the transaction hash;~~

~~determining the concealed data based on data obtained by concatenating the to generate a first concatenation, wherein the header is at a front marking character and of the transaction hash; and~~

~~replacing, with the 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 transactions;~~

~~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 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.~~

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

~~11. The apparatus 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,
5 wherein ~~the determining~~identifying the concealed data based on ~~data obtained by concatenating the front marking character and the transaction hash specifically comprises the following~~the first concatenation comprising:

concatenating a predetermined rear marking character to an end of the ~~transaction hash, and~~first concatenation;

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

~~determining, as the concealed data, data obtained by concatenating the front marking character, the transaction hash, the rear marking character, and the remark information.~~

~~12. identifying the second concatenation as the concealed data.~~

12. The apparatus~~non-transitory, computer-readable medium~~ according to
20 claim 10 ~~or 11~~, wherein ~~the analysis module is configured to: if~~analyzing the data ~~read~~retrieved from the transaction storage ~~position~~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
25 storage location does not comprise the front marking character, ~~determine, as the transaction, the data read from the transaction storage position; or if the data read~~identifying the data retrieved from the transaction storage ~~position~~comprises the front marking character, determine, as the concealed data, the data readlocation as the transaction; and

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

~~13.~~

13. ~~The apparatus~~non-transitory, computer-readable medium according to claim 10, wherein extracting the transaction hash ~~determination module is configured to determine~~from the concealed data comprises:

identifying information located after the front marking character in the concealed data as the transaction hash ~~and extract the transaction hash;~~ and
14. ~~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 apparatus~~non-transitory, computer-readable medium according to claim 11, wherein extracting the transaction hash ~~determination module is configured to determine~~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 extract the transaction hash;~~ and

15. ~~An SPV apparatus~~extracting the transaction hash, wherein the ~~apparatus is any full node in a blockchain network, and~~ transaction hash comprises ~~the following:~~ a hash value obtained from performing a hash operation on a corresponding transaction only.

a

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

~~receiving module, configured to receive a, by the full node, the~~ verification request, wherein the verification request comprises a target transaction identifier of the target transaction;

~~a determination and construction module, configured to determine~~identifying, in ~~a~~ the blockchain ~~of~~associated with the ~~SPV apparatus~~full node based on the verification request, ~~a~~ the block ~~that ain which the target~~ transaction corresponding to the target transaction identifier is located ~~in, and construct a Merkle tree corresponding to the block based on the method according to any one of claims 1 to 6;~~ and

~~a triggering module, configured to trigger an SPV~~ the simplified payment verification (SPV) procedure for the target transaction corresponding to the target

transaction identifier based on the ~~constructed~~ Merkle tree path to the target transaction.

16. ~~The apparatus~~ The non-transitory, computer-readable medium
5 according to claim 15, wherein ~~for any transaction written to the blockchain, a~~
correspondence between a transaction identifier of the transaction and ~~a~~ the transaction
storage ~~position~~ location of the transaction in the blockchain is pre-~~recorded on each~~
~~node stored in the each of the blockchain network, and wherein identifying the block in~~
~~the blockchain network; and~~ which the transaction corresponding to the target
10 transaction identifier is located comprises:

identifying the ~~determination and construction module is configured to~~
~~determine a~~ transaction storage ~~position~~ location corresponding to the target transaction
identifier as a target transaction storage ~~position~~ location based on the correspondence;
and

15 identifying the block that comprises the target transaction ~~identifier and a pre-~~
~~recorded correspondence between~~ storage location as the block in which the transaction
is located.

17. ~~identifier~~ A computer-implemented system, comprising:

20 one or more computers; and ~~the~~

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:

25 for each transaction storage ~~position; and determine, as the block that the~~
~~transaction corresponding to the location in a~~ target transaction identifier is located
~~in, block of~~ a ~~block~~ blockchain network that comprises ~~the target transaction storage~~
~~position~~ a full node and a light node, retrieving, by the

~~17. A blockchain system, comprising a blockchain network comprising a plurality~~
30 ~~of nodes, wherein~~

~~for each transaction storage position in a target block, any full node in the~~
blockchain network ~~reads,~~ data from ~~the~~ a respective transaction storage ~~position,~~

~~wherein the target block is any block in a blockchain of a target full node;
analyzes~~location;

~~analyzing the data read~~retrieved from the each transaction storage ~~position;~~ if
~~it is determined that~~location;

5 ~~determining, for each transaction storage location, whether the data~~
~~read~~retrieved from the respective transaction storage ~~position~~location is ~~a~~-transaction;
~~performs 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; ~~or if it is determined~~

10 ~~in response to determining that the data read from the transaction storage~~
~~position~~retrieved is concealed data, ~~extracts a~~extracting the transaction hash from
the concealed data, wherein the transaction hash ~~extracted from the concealed data~~
is a hash value of the transaction ~~hash of a transaction originally~~ stored at the
transaction storage ~~position; an operation of replacing;~~location, and each node in the
15 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 originally~~hash of the transaction stored at the
transaction storage ~~position is performed by a node having a transaction concealment~~
20 ~~permission in the blockchain network by instructing each node; and constructs~~
~~a~~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~~
25 ~~hash;~~hash;

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

18. ~~A blockchain system, comprising a blockchain network comprising a plurality~~
30 ~~of nodes, wherein~~

~~any full node in the blockchain network receives~~response to receiving a
verification request, ~~wherein the verification request comprises a~~ of a target
transaction ~~identifier; determines, in a blockchain of the full node;~~

determining, from the Merkle tree that has been generated based on the verification request, a block that a transaction corresponding or the concealed data or both, a Merkle tree path to the target transaction identifier is located in;

computing a hash value associated with the Merkle tree path to the target transaction; and ~~constructs a Merkle tree corresponding to the block based on the method according to any one of claims 1 to 6; and triggers an SPV procedure for~~
providing the hash value associated with the transaction corresponding Merkle tree path to the target transaction identifier based on the constructed Merkle tree 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~~19. ~~A computer device, comprising a memory, a processor, and a computer program stored in the memory and capable of running on the processor, wherein when the processor executes the program, the method according to any one of claims 1 to 6 is performed.~~ 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 data.

~~20.~~ 21. ~~A computer device, comprising a memory, a processor, and a computer program stored in the memory and capable of running on the processor, wherein when the processor executes the program, the method according to claim 7 or 8 is performed.~~ 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;

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.

20. -

- 5 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;
- in response to determining that the data retrieved from the transaction storage
location does not comprise the front marking character, identifying the data retrieved
10 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.