

CLAIMS

What is claimed is:

1. A method for retrieving blockchain data, comprising:
 - receiving, by a node in a blockchain network, a data retrieving request that
 - 5 comprises a target transaction identifier;
 - identifying, by the node, a transaction storage location that corresponds to the target transaction identifier as a target transaction storage location based on a pre-stored correspondence between transaction identifiers of transactions recorded on a blockchain associated with the blockchain network and transaction storage locations
 - 10 of the transactions; and
 - retrieving data from the target transaction storage location in the blockchain, wherein the data is concealed data that replaces a target transaction identified by the target transaction identifier and originally stored in the target transaction storage location, wherein the concealed data comprises a transaction hash of the target
 - 15 transaction, wherein replacing the target transaction identified by the target transaction identifier comprises:
 - obtaining the transaction hash of the target transaction;
 - concatenating a predetermined front marking character to a header of the transaction hash to generate a first concatenation;
 - 20 identifying the concealed data based on the first concatenation; and
 - replacing the target transaction with the concealed data.
2. The method of claim 1, wherein replacing the target transaction identified by the target transaction identifier with the concealed data is instructed by a separate
- 25 node in the blockchain network that has a transaction concealment permission to other nodes in the blockchain network.
3. The method according to claim 1, wherein identifying the concealed data based on the first concatenation comprises:
 - 30 concatenating a predetermined rear marking character to an end of the first concatenation to generate a second concatenation; and
 - identifying the second concatenation as the concealed data.

4. The method according to claim 1, further comprising:
determining, by the node, that the retrieved data comprises the predetermined
front marking character; and

5 providing an indication, by the node in response to the data retrieving request,
that the target transaction is replaced with the concealed data.

5. The method according to claim 1, further comprising:
sending, by the node, the retrieved data in response to the data retrieving
10 request.

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

receiving, by a node in a blockchain network, a data retrieving request that
15 comprises a target transaction identifier;

identifying, by the node, a transaction storage location that corresponds to the
target transaction identifier as a target transaction storage location based on a
pre-stored correspondence between transaction identifiers of transactions recorded on
a blockchain associated with the blockchain network and transaction storage locations
20 of the transactions; and

retrieving data from the target transaction storage location in the blockchain,
wherein the data is concealed data that replaces a target transaction identified by the
target transaction identifier and originally stored in the target transaction storage
location, wherein the concealed data comprises a transaction hash of the target
25 transaction, wherein replacing the target transaction identified by the target
transaction identifier comprises:

obtaining the transaction hash of the target transaction;
concatenating a predetermined front marking character to a header of the
transaction hash to generate a first concatenation;
30 identifying the concealed data based on the first concatenation; and
replacing the target transaction with the concealed data.

7. The non-transitory, computer-readable medium of claim 6, wherein
replacing the target transaction identified by the target transaction identifier with the

concealed data is instructed by a separate node in the blockchain network that has a transaction concealment permission to other nodes in the blockchain network.

8. The non-transitory, computer-readable medium according to claim 6, wherein
5 identifying the concealed data based on the first concatenation comprises:
concatenating a predetermined rear marking character to an end of the first
concatenation to generate a second concatenation; and
identifying the second concatenation as the concealed data.

10 9. The non-transitory, computer-readable medium according to claim 6, the
operations further comprising:
determining, by the node, that the retrieved data comprises the predetermined
front marking character; and
providing an indication, by the node in response to the data retrieving request,
15 that the target transaction is replaced with the concealed data.

10. The non-transitory, computer-readable medium according to claim 6, the
operations further comprising:
sending, by the node, the retrieved data in response to the data retrieving
20 request.

11. A computer-implemented system, comprising:
one or more computers; and
one or more computer memory devices interoperably coupled with the one or
25 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:
receiving, by a node in a blockchain network, a data retrieving request that
comprises a target transaction identifier;
30 identifying, by the node, a transaction storage location that corresponds to the
target transaction identifier as a target transaction storage location based on a
pre-stored correspondence between transaction identifiers of transactions recorded on
a blockchain associated with the blockchain network and transaction storage locations
of the transactions; and

retrieving data from the target transaction storage location in the blockchain,
wherein the data is concealed data that replaces a target transaction identified by the
target transaction identifier and originally stored in the target transaction storage
location, wherein the concealed data comprises a transaction hash of the target
5 transaction, wherein replacing the target transaction identified by the target
transaction identifier comprises:

obtaining the transaction hash of the target transaction;
concatenating a predetermined front marking character to a header of the
transaction hash to generate a first concatenation;
10 identifying the concealed data based on the first concatenation; and
replacing the target transaction with the concealed data.

12. The computer-implemented system of claim 11, wherein replacing the target
transaction identified by the target transaction identifier with the concealed data is
15 instructed by a separate node in the blockchain network that has a transaction
concealment permission to other nodes in the blockchain network.

13. The computer-implemented system according to claim 11, wherein
identifying the concealed data based on the first concatenation comprises:
20 concatenating a predetermined rear marking character to an end of the first
concatenation to generate a second concatenation; and
identifying the second concatenation as the concealed data.

14. The computer-implemented system according to claim 11, the one or more
25 operations further comprising:
determining, by the node, that the retrieved data comprises the predetermined
front marking character; and
providing an indication, by the node in response to the data retrieving request,
that the target transaction is replaced with the concealed data.

30 15. The computer-implemented system according to claim 11, the one or more
operations further comprising:
sending, by the node, the retrieved data in response to the data retrieving request.