CLAIMS

1. A transaction uploading method, performed by a first relay node, the method comprising:

determining, when a first consensus node in a local consensus network receives a local transaction, a parent type of the local transaction, wherein a global consensus network comprises a first global consensus network and a second global consensus network;

instructing, when the parent type is a second type, the first consensus node to execute the local transaction and to record the local transaction to a first blockchain, the first blockchain being accessible by nodes other than the first consensus node;

transmitting, when the parent type is a first type, the local transaction to a second consensus node in the first global consensus network, the local transaction being used for instructing the second consensus node to execute the local transaction for recording the local transaction to a second blockchain, generate first uploading verification information of the local transaction, and transmit the first uploading verification information to a third consensus node in the second global consensus network, wherein

the first uploading verification information is used for instructing the third consensus node to verify uploading of the local transaction according to the first uploading verification information to obtain an uploading verification result of the local transaction;

the second blockchain is not accessible by nodes other than the second consensus node;

the first uploading verification information comprises transaction desensitization information, the transaction desensitization information comprising information in the local transaction that is able to be disclosed to a third party; and

obtaining the transaction desensitization information from the third consensus node as the uploading verification result.

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

obtaining a global transaction generalized from a plurality of local transactions of the second type; and

transmitting the global transaction to the third consensus node, the global transaction being used for instructing the third consensus node to execute the global transaction and to record the global transaction to a third blockchain, and the third blockchain being accessible by nodes other

than the third consensus node.

3. The method according to claim 2, further comprising:

receiving, when the third consensus node records the global transaction to the third blockchain to generate second uploading verification information, the second uploading verification information from the third consensus node; and

transmitting the second uploading verification information to the first consensus node, the second uploading verification information being used for instructing the first consensus node to verify uploading of the global transaction.

4. The method according to any one of claims 1 to 3, wherein the first uploading verification information further comprises a digest value of the local transaction and a digest value that is determined according to a first path in a first tree and recorded in a first bypass node; a leaf node in the first tree records a digest value of a transaction recorded on the second blockchain; the first path is a path from a leaf node in the first tree to a root node in the first tree, and the leaf node in the first tree records the digest value of the local transaction; the first bypass node is a sibling node in the first tree of nodes other than the root node in the first path; the first uploading verification information is further used for instructing the third consensus node to determine a first comparative digest value according to the digest value of the local transaction and the digest value recorded in the first bypass node; and verification is successful when the digest value recorded in the root node in the first tree and the first comparative digest value are consistent.

5. The method according to claim 4, wherein the first uploading verification information further comprises a digest value of associated data obtained after execution of the local transaction and a digest value recorded in a second bypass node in a second tree; a leaf node in the second tree records a digest value of associated data obtained after execution of a transaction recorded on the second blockchain; a second path is a path from a leaf node in the second tree to a root node in the second tree, and the leaf node in the second tree records the digest value of the associated data obtained after execution of the local transaction; the second bypass node is a sibling node in the second tree of nodes other than the root node on the second path; the first uploading verification information is further used for instructing the third consensus node to determine, when the digest value recorded in the root node in the first tree and the first comparative digest value are consistent, a second comparative digest value according to the digest value of the associated data obtained after execution of the local transaction and the digest value recorded in the second bypass node; and the verification is successful when the digest value recorded in the root node in the second tree and the second comparative digest value are consistent.

6. The method according to claim 1, wherein the transaction desensitization information is obtained by desensitizing the local transaction by the second consensus node, the desensitization is performed according to a desensitization field in a target contract, and the target contract corresponds to a child type of the local transaction.

7. The method according to claim 5, wherein the first uploading verification information further comprises a first signature of the second bypass node, the first signature is obtained by encrypting a first digest by the second consensus node with a first private key of the second consensus node, and the first digest is generated by the second consensus node according to the digest value of the local transaction, the digest value recorded in the first bypass node, the digest value of the associated data obtained after execution of the local transaction, and the digest value recorded in the second bypass node; and

the first signature is used for instructing the third consensus node to decrypt, when the root node in the second tree is consistent with a second to-be-compared root node, the first signature with a first public key of the second consensus node to obtain a second digest, and to generate a third digest according to the digest value of the local transaction, the digest value recorded in the first bypass node, the digest value of the associated data obtained after execution of the local transaction, and the digest value recorded in the second bypass node, and the verification is successful when the third digest and the second digest are consistent.

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

receiving a block identifier returned by the third consensus node after the third consensus node records a block comprising the uploading verification result to a third blockchain, the block identifier referring to the block comprising the uploading verification result,

transmitting an uploading verification result request to the third consensus node, the uploading verification result request carrying the block identifier, and the uploading verification result request being used for instructing the third consensus node to obtain the uploading verification result from the third blockchain according to the block identifier.

9. The method according to any one of claims 1 to 8, wherein the transmitting, when the parent type is a first type, the local transaction to a second consensus node in the first global consensus network comprises:

placing the local transaction in a queue for queuing; and

packaging local transactions in the queue in response to the queue satisfying a predetermined condition, and transmitting the local transaction to the second consensus node.

10. The method according to claim 9, wherein the packaging local transactions in the queue in response to the queue satisfying a predetermined condition comprises:

packaging local transactions in the queue in response to the number of local transactions in the queue reaching a first threshold.

11. The method according to claim 9, wherein the packaging local transactions in the queue in response to the queue satisfying a predetermined condition comprises:

determining a time difference between a current time and a previous packaging time in response to the number of local transactions in the queue not reaching a first threshold; and

packaging local transactions in the queue in response to the time difference reaching a second threshold.

12. The method according to claim 9, wherein the placing the local transaction in a queue for queuing comprises:

determining a child type of the local transaction;

determining a queue corresponding to the child type of the local transaction; and

placing the local transaction in the queue corresponding to the child type for queuing.

13. The method according to claim 12, wherein the packaging local transactions in the queue in response to the queue satisfying a predetermined condition comprises:

packaging local transactions in the queue in response to the number of local transactions in the queue reaching a third threshold.

14. The method according to any one of claims 1 to 8, wherein the transmitting, when the parent type is a first type, the local transaction to a second consensus node in the first global consensus network comprises:

determining a child type of the local transaction;

determining a priority of the local transaction according to the child type;

placing the local transaction in a queue for queuing in a descending order of priority; and

sequentially taking out the local transactions from the queue, and transmitting the local transactions to the second consensus node.

15. The method according to any one of claims 1 to 14, wherein the second consensus node has a trusted execution environment (TEE), and the second blockchain is encrypted with a key of the TEE; the first uploading verification information is transmitted by the second consensus node to

a second relay node in response to a first uploading verification information request transmitted by the second relay node, the first uploading verification information request is transmitted by the second relay node in response to adding an encrypted block on the second blockchain, the encrypted block is encrypted with the key of the TEE, and the first uploading verification information is used for instructing the second relay node to forward the first uploading verification information to the third consensus node.

16. A transaction uploading method, performed by a second consensus node in a first global consensus network, the method comprising:

receiving a local transaction forwarded by a first relay node, a parent type of the local transaction being a first type, wherein

when the parent type is a second type, the first relay node instructs a first consensus node in a local consensus network to execute the local transaction and to record the local transaction to a first blockchain, the first blockchain being accessible by nodes other than the first consensus node;

a global consensus network comprises the first global consensus network and a second global consensus network;

executing the local transaction, and recording the local transaction to a second blockchain, the second blockchain being not accessible by nodes other than the second consensus node;

generating first uploading verification information of the local transaction; and

transmitting the first uploading verification information to a third consensus node in the second global consensus network, wherein

the first uploading verification information is used for instructing the third consensus node to verify uploading of the local transaction according to the first uploading verification information to obtain an uploading verification result of the local transaction;

the first uploading verification information comprises transaction desensitization information, the transaction desensitization information comprising information in the local transaction that is able to be disclosed to a third party; and

the first relay node obtains the transaction desensitization information from the third consensus node as the uploading verification result.

17. The method according to claim 16, wherein the second consensus node has a trusted execution environment (TEE), and the second blockchain is encrypted with a key of the TEE; and

the transmitting the first uploading verification information to a third consensus node in the

second global consensus network comprises:

receiving a first uploading verification information request transmitted by a second relay node, the first uploading verification information request being transmitted by the second relay node in response to adding an encrypted block on the second blockchain, and the encrypted block being encrypted with the key of the TEE; and

transmitting the first uploading verification information to the second relay node in response to the first uploading verification information request, the first uploading verification information being used for instructing the second relay node to forward the first uploading verification information to the third consensus node.

18. A transaction uploading apparatus, comprising:

a first determining unit, configured to determine, when a first consensus node in a local consensus network receives a local transaction, a parent type of the local transaction, wherein a global consensus network comprises a first global consensus network and a second global consensus network;

a first transmitting unit, configured to instruct, when the parent type is a second type, the first consensus node to execute the local transaction and to record the local transaction to a first blockchain, the first blockchain being accessible by nodes other than the first consensus node; transmit, when the parent type is a first type, the local transaction to a second consensus node in the first global consensus network, the local transaction being used for instructing the second consensus node to execute the local transaction for recording the local transaction to a second blockchain, generate first uploading verification information of the local transaction, and transmit the first uploading verification information of the local transaction to a third consensus node in the second global consensus network, wherein the first uploading verification information is used for instructing the third consensus node to verify uploading of the local transaction according to the first uploading verification information to obtain an uploading verification result of the local transaction, and the second blockchain is not accessible by nodes other than the second consensus node; the first uploading verification information comprises transaction desensitization information, the transaction desensitization information comprising information in the local transaction that is able to be disclosed to a third party; and

a first obtaining unit, configured to obtain the transaction desensitization information from the third consensus node as the uploading verification result.

19. A transaction uploading apparatus in a first global consensus network, comprising:

a first receiving unit, configured to receive a local transaction forwarded by a first relay node, a parent type of the local transaction being a first type, wherein

when the parent type is a second type, the first relay node instructs a first consensus node in a local consensus network to execute the local transaction and to record the local transaction to a first blockchain, the first blockchain being accessible by nodes other than the first consensus node;

a global consensus network comprises the first global consensus network and a second global consensus network;;

a second uploading unit, configured to execute the local transaction, and record the local transaction to a second blockchain, the second blockchain being not accessible by nodes other than the second consensus node;

a second obtaining unit, configured to generate first uploading verification information of the local transaction; and

a second transmitting unit, configured to transmit the first uploading verification information to a third consensus node in the second global consensus network, wherein

the first uploading verification information is used for instructing the third consensus node to verify uploading of the local transaction according to the first uploading verification information to obtain an uploading verification result of the local transaction;

the first uploading verification information comprises transaction desensitization information, the transaction desensitization information comprising information in the local transaction that is able to be disclosed to a third party; and

the first relay node obtains the transaction desensitization information from the third consensus node as the uploading verification result.

20. An electronic device, comprising a memory and one or more processors, the memory storing computer-readable instructions, the processor, when executing the computer-readable instructions, implementing the transaction uploading method according to any one of claims 1 to 17.

21. One or more readable storage media, storing computer-readable instructions, the computer-readable instructions, when executed by one or more processors, implementing the transaction uploading method according to any one of claims 1 to 17.

22. A computer program product, comprising computer-readable instructions, the computer-readable instructions being read and executed by one or more processors of a computer device, whereby the computer device performs the transaction uploading method according to any

one of claims 1 to 17.