

CLAIMS

What is claimed is:

1. A data processing method, comprising:

determining, by a transaction initiator, information to be hidden in transaction data;

determining pre-transaction data and post-transaction data in the transaction data;

~~obtaining, by using the pre-transaction data as an input of a first predetermined one-way function, an input transaction root that is output by the first predetermined one-way function;~~
~~by:~~

obtaining, by using the pre-transaction data as an input of a first predetermined one-way function, an input transaction root that is output by the first predetermined one-way function;

obtaining, by using the post-transaction data as an input of a second predetermined one-way function, an output transaction root that is output by the second predetermined one-way function;

using the input transaction root and the output transaction root as transaction roots for adding to a blockchain;

constructing, according to the input transaction root and the output transaction root, proof data of validity of the information to be hidden; and

initiating a transaction request to write the proof data and the input transaction root and the output transaction root carrying a signature of the transaction initiator on the blockchain, for a plurality of nodes in the blockchain to perform consensus verification on the input transaction root, the output transaction root, and the proof data, and approve or reject the transaction request according to a verification result.

2. The method according to claim 1, wherein the obtaining, by using the post-transaction data as an input of a second predetermined one-way function, an output transaction root that is output by the second predetermined one-way function comprises:

constructing, according to the post-transaction data and a random number, a bottom layer of a predetermined one-way function tree, and

determining the output transaction root corresponding to a top layer of the predetermined one-way function tree.

3. The method according to claim 1, wherein the constructing, according to the input transaction root and the output transaction root, proof data of validity of the information to be

hidden comprises:

performing, by using the input transaction root, the output transaction root, and the information to be hidden as inputs, a predetermined logical operation; and

performing, by using the information to be hidden as a protected object, a zero-knowledge proof on the logical operation to obtain the proof data.

4. A data processing method, comprising:

receiving a transaction request from a transaction initiator, wherein the transaction request is used to request to write a transaction root and proof data on a blockchain, the transaction root is based on transaction data as an input of a predetermined one-way function, and the proof data is used to prove information to be hidden in the transaction data;

performing verification on the transaction root, to obtain a first verification result, by verifying whether an output transaction root and an input transaction root in the transaction root is the same as a stored output transaction root and a stored input transaction root on the blockchain, wherein the output transaction root is based on post-transaction data in the transaction data as an input of a first predetermined one-way function, and wherein the input transaction root is based on pre-transaction data in the transaction data as an input of a second predetermined one-way function;

performing, according to the transaction root, verification on the proof data to obtain a second verification result; and

approving or rejecting the transaction request according to the first verification result and the second verification result.

5. The method according to claim 4, wherein the performing verification on the transaction root comprises:

verifying whether the transaction root has a valid signature.

6. The method according to claim 5, wherein the verifying whether the transaction root has a valid signature comprises:

determining an address associated with the output transaction root in the transaction root; and

verifying, if determining that a quantity of obtained addresses is 1, whether the transaction root has a signature corresponding to the transaction initiator.

7. The method according to claim 4, wherein the approving or rejecting the transaction request according to the first verification result and the second verification result comprises:

if the first verification result and the second verification result both are successful, writing, in response to the transaction request, the transaction root carrying a signature of the transaction initiator and the proof data on the blockchain; or

if the first verification result and/or the second verification result is failed, rejecting the transaction request.

8. A data processing method, comprising:

determining, by a transaction initiator, information to be hidden in transaction data;

determining pre-transaction data and post-transaction data in the transaction data;

obtaining, by using the pre-transaction data as an input of a first predetermined one-way function, an input transaction root that is output by the first predetermined one-way function;

obtaining, by using the post-transaction data as an input of a second predetermined one-way function, an output transaction root that is output by the second predetermined one-way function;

using the input transaction root and the output transaction root as transaction roots for adding to a blockchain;

constructing, according to the input transaction root and the output transaction root, proof data of validity of the information to be hidden; and

sending the input transaction root, the output transaction root, and the proof data to a transaction receiver, wherein the transaction receiver performs verification on the input transaction root and the output transaction root, and initiates, after the verification succeeds, a transaction request to write the proof data, the input transaction root, and the output transaction root carrying signatures of the transaction initiator and the transaction receiver on the blockchain.

9. A data processing method, comprising:

receiving, by a transaction receiver, a transaction root and proof data from a transaction sender, wherein the transaction root includes an input transaction root and an output transaction root, wherein the input transaction root is obtained by using the pre-transaction data as an input of a first predetermined one-way function, and the output transaction root is obtained by using the post-transaction data as an input of a second predetermined one-way function, and the proof data is used to prove information to be hidden in the transaction data;

performing verification on the transaction root according to the information to be hidden and the first and second predetermined one-way functions; and

if a verification result is successful, initiating a transaction request to write the proof data and the transaction root carrying signatures of the transaction initiator and the transaction receiver on a blockchain, for a node in the blockchain to perform consensus verification on the transaction root and the proof data, and approve or reject the transaction request according to a verification result.

10. A data processing method, comprising:

receiving a transaction request from a transaction receiver, wherein: the transaction request is used to request to write a transaction root and proof data on a blockchain, the transaction root includes an input transaction root and an output transaction root, wherein the input transaction root is obtained by using the pre-transaction data as an input of a first predetermined one-way function, and the output transaction root is obtained by using the post-transaction data as an input of a second predetermined one-way function, and the proof data is used to prove information to be hidden in the transaction data;

performing verification on the transaction root to obtain a first verification result;

performing, according to the transaction root, verification on the proof data to obtain a second verification result; and

approving or rejecting the transaction request according to the first verification result and the second verification result.

11. The method according to claim 10, wherein the performing verification on the transaction root comprises:

determining an address associated with the output transaction root in the transaction root; and

if determining that a quantity of obtained addresses is greater than or equal to a predetermined threshold, verifying whether the transaction root carries signatures corresponding to the transaction initiator and the transaction receiver.

12. An apparatus comprising:

one or more processors; and

a memory storing instructions executable by the one or more processors to cause the one or more processors to perform operations comprising:

determining, by a transaction initiator, information to be hidden in transaction data;
determining pre-transaction data and post-transaction data in the transaction data;
obtaining, by using the pre-transaction data as an input of a first predetermined one-way function, an input transaction root that is output by the first predetermined one-way function;
obtaining, by using the post-transaction data as an input of a second predetermined one-way function, an output transaction root that is output by the second predetermined one-way function;
using the input transaction root and the output transaction root as transaction roots for adding to a blockchain;
constructing, according to the input transaction root and the output transaction root, proof data of validity of the information to be hidden; and
initiating a transaction request to write the proof data and the input transaction root and the output transaction root carrying a signature of the transaction initiator on the blockchain, for a plurality of nodes in the blockchain to perform consensus verification on the input transaction root, the output transaction root, and the proof data, and approve or reject the transaction request according to a verification result.

13. The method according to claim 12, wherein the obtaining, by using the post-transaction data as an input of a second predetermined one-way function, an output transaction root that is output by the second predetermined one-way function comprises:

constructing, according to the post-transaction data and a random number, a bottom layer of a predetermined one-way function tree, and
determining the output transaction root corresponding to a top layer of the predetermined one-way function tree.

14. The method according to claim 12, wherein the constructing, according to the input transaction root and the output transaction root, proof data of validity of the information to be hidden comprises:

performing, by using the input transaction root, the output transaction root, and the information to be hidden as inputs, a predetermined logical operation; and
performing, by using the information to be hidden as a protected object, a zero-knowledge proof on the logical operation to obtain the proof data.

15. An apparatus comprising:
one or more processors; and
a memory storing instructions executable by the one or more processors to cause the one or more processors to perform operations comprising:
receiving a transaction request from a transaction initiator, wherein the transaction request is used to request to write a transaction root and proof data on a blockchain, the transaction root is based on transaction data as an input of a predetermined one-way function, and the proof data is used to prove information to be hidden in the transaction data;
performing verification on the transaction root, to obtain a first verification result, by verifying whether an output transaction root and an input transaction root in the transaction root is the same as a stored output transaction root and a stored input transaction root on the blockchain, wherein the output transaction root is based on post-transaction data in the transaction data as an input of a first predetermined one-way function, and wherein the input transaction root is based on pre-transaction data in the transaction data as an input of a second predetermined one-way function;
performing, according to the transaction root, verification on the proof data to obtain a second verification result; and
approving or rejecting the transaction request according to the first verification result and the second verification result.

16. The method according to claim 15, wherein the performing verification on the transaction root comprises:
verifying whether the transaction root has a valid signature.

17. The method according to claim 16, wherein the verifying whether the transaction root has a valid signature comprises:
determining an address associated with the output transaction root in the transaction root;
and
verifying, if determining that a quantity of obtained addresses is 1, whether the transaction root has a signature corresponding to the transaction initiator.

18. The method according to claim 15, wherein the approving or rejecting the transaction request according to the first verification result and the second verification result comprises:
if the first verification result and the second verification result both are successful, writing,

in response to the transaction request, the transaction root carrying a signature of the transaction initiator and the proof data on the blockchain; or

if the first verification result and/or the second verification result is failed, rejecting the transaction request.