

CLAIMS

1. A computer-implemented method for consensus verification, the computer-implemented method comprising:

receiving, by a regulatory node, a transaction request, wherein the transaction request comprises transaction data and a signature of at least one transaction node, the transaction data comprises specified data and non-specified data, and the specified data comprises privacy data;

determining an asset number that corresponds to the signature of the at least one transaction node in the transaction data based on the signature;

determining the asset number as a declared asset number used by the at least one transaction node;

determining whether the transaction request is valid based on the transaction data, the signature, and the asset number, wherein determining whether the transaction request is valid based on the transaction data, the signature, and the asset number comprises determining whether the transaction request is valid based on determining whether the declared asset number used by the at least one transaction node is actually owned by the at least one transaction node;

in response to determining that the transaction request is valid, generating a digest of the specified data based on the specified data comprised in the transaction data; and

sending the digest of the specified data and the non-specified data and not sending the specified data comprised in the transaction data to a respective consensus node, so that a consensus verification of the transaction data is performed based on the digest of the specified data and the non-specified data.

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

rejecting the transaction request in response to determining that the transaction request is invalid.

3. The computer-implemented method according to claim 1, wherein before determining whether the transaction request is valid comprises:

obtaining a digital certificate of the at least one transaction node.

4. The computer-implemented method according to claim 3, wherein determining whether the transaction request is valid comprises:

determining whether the transaction request is valid based on the transaction data, the signature of the at least one transaction node, and the digital certificate of the at least one transaction node.

5. The computer-implemented method according to claim 3, wherein determining whether the transaction request is valid comprises:

decrypting the signature of the at least one transaction node based on a public key comprised in the digital certificate of the transaction node;

determining whether a decryption result that corresponds to the at least one transaction node corresponds to a digest of the transaction data;

in response to determining that the decryption result that corresponds to the at least one transaction node corresponds to the digest of the transaction data, determining one or more asset numbers that correspond to an identity based on the identity comprised in the digital certificate of the at least one transaction node; and

determining the one or more asset numbers as one or more asset numbers actually owned by the transaction node.

6. The computer-implemented method according to claim 5, further comprising:

determining whether the transaction request is valid based on the one or more asset numbers owned by the at least one transaction node, the signature of the at least one transaction node, and the transaction data; or

determining that the transaction request is invalid in response to determining that a decryption result that corresponds to the at least one transaction node is different from the digest of the transaction data.

7. The computer-implemented method according to claim 6, wherein determining whether the transaction request is valid comprises:

determining that the transaction node is invalid in response to determining that the one or more asset numbers owned by the transaction node do not comprise the declared asset number used by the transaction node; or

determining that the transaction node is valid in response to determining that the one or more asset numbers owned by the transaction node comprises all declared asset numbers used by the transaction node.

8. The computer-implemented method according to claim 1, wherein determining whether the transaction request is valid comprises:

determining that the transaction request is invalid in response to determining that at least one transaction node is invalid; or

determining that the transaction request is valid in response to determining that all transaction nodes identified in the transaction request are valid.

9. The computer-implemented method according to claim 1, further comprising:

instructing the at least one transaction node to store the transaction data or the specified data comprised in the transaction data in response to determining that the transaction request is valid.

10. The computer-implemented method according to claim 1, wherein the regulatory node is a node of a blockchain network configured to regulate transactions by verifying items, wherein the items verified by the regulatory node are acknowledged by a plurality of blockchain nodes of the blockchain network.

11. The computer-implemented method according to claim 10, wherein the blockchain network comprises a consortium blockchain network.

12. A device for consensus verification, the device comprising a plurality of modules configured to perform the computer-implemented method of any one of claims 1 to 11.