

CLAIMS

1. A method for consensus verification, the method comprising:

obtaining, by a regulatory node, a transaction request, wherein the transaction request comprises transaction data and a signature of at least one transaction node;

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

assigning the asset number to the at least one transaction node;

determining whether the transaction request is valid based on the transaction data, the signature, and the asset number;

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

sending the digest and non-specified data comprised in the transaction data to a respective consensus node, so that the respective consensus node performs a consensus verification.

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

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

3. The 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 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 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;

in response to determining that a decryption result that corresponds to the at least one transaction node is same as the digest of the transaction data, determining the asset number that corresponds to an identity based on the identity comprised in the digital certificate of the at least one transaction node; and

determining the asset number as a transaction asset number owned by the transaction node.

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

determining whether the transaction request is valid based on the asset number 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 when determining that a decryption result that corresponds to at least one transaction node is different from the digest of the transaction data.

7. The 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 asset number owned by the transaction node does not comprise at least one asset number used by the transaction node; or

determining that the transaction node is valid in response to determining that the asset number owned by the transaction node comprises all asset numbers used by the transaction node.

8. The method according to claim 7, 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 are valid.

9. The 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 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 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 method of any one of claims 1 to 11.