

Claims

1. A method comprising:

before a consensus verification phase begins:

performing, by a first blockchain node, an asymmetric signature legality verification on a blockchain transaction;

in response to determining that the blockchain transaction passes the asymmetric signature legality verification:

storing, by the first blockchain node, the blockchain transaction; and

broadcasting, by the first blockchain node, the blockchain transaction to each of a plurality of second blockchain nodes;

generating, by the first blockchain node, a pre-processed data block comprising an identifier of the blockchain transaction that has passed the asymmetric signature legality verification and has been broadcast to the plurality of second blockchain nodes; and

during the consensus verification phase:

broadcasting, by the first blockchain node, the pre-processed data block to each of the plurality of second blockchain nodes.

2. The method according to claim 1, wherein:

the first blockchain node further comprises a routing device; and

performing the asymmetric signature legality verification on the blockchain transaction comprises selecting, by the routing device, a server according to load balancing and performing, by the server, the asymmetric signature legality verification on the blockchain transaction

3. The method according to claim 2, wherein the routing device comprises a load-balancing device.

4. The method according to claim 1, wherein:

the first blockchain node further comprises a gateway; and

performing the asymmetric signature legality verification on the blockchain transaction comprises selecting, by the gateway, a server according to load balancing and performing, by the server, the asymmetric signature legality verification on the blockchain transaction.

5. The method according to claim 1, wherein performing the asymmetric signature legality verification on the blockchain transaction comprises:

obtaining a public key of a public-private key pair of a user, wherein the blockchain transaction is encrypted with a private key of the public-private key pair;

obtaining decrypted information of the blockchain transaction by decrypting the blockchain transaction with the public key; and

verifying the decrypted information of the blockchain transaction.

6. The method according to claim 1, wherein generating the pre-processed data block comprises:

determining a plurality of sub-hash values of a plurality of blockchain transactions according to a hash algorithm, the plurality of blockchain transactions comprising the received blockchain transaction;

generating a hash value according to an order of a queue of identifiers of the plurality of blockchain transactions; and

packaging the generated hash value and the queue of the plurality of identifiers in the order into the pre-processed data block.

7. The method according to claim 1, wherein:

before generating, by the first blockchain node, the pre-processed data block, the method further comprises transferring the plurality of blockchain transactions from the memory to a server, or marking the plurality of blockchain transactions in the memory; and

generating, by the first blockchain node, the pre-processed data block comprises generating, by the server, the pre-processed data block.

8. A method comprising:

before a consensus verification phase begins:

receiving, by a second blockchain node, a blockchain transaction broadcast by a first blockchain node;

performing, by the second blockchain node, an asymmetric signature legality verification on the blockchain transaction; and

in response to the second blockchain node determining that the blockchain transaction passes the asymmetric signature legality verification, storing, by the second blockchain node, the

blockchain transaction; and

during the consensus verification phase:

receiving, by the second blockchain node, a pre-processed data block broadcast by the first blockchain node, wherein the pre-processed data block comprises an identifier of the blockchain transaction that has passed the asymmetric signature legality verification and has been stored at the second blockchain node; and

performing, by the second blockchain node, consensus verification on the pre-processed data block.

9. The method according to claim 8, wherein:

the second blockchain node further comprises a routing device; and

performing the asymmetric signature legality verification on the blockchain transaction comprises selecting, by the routing device, a server according to load balancing and performing, by the server, the asymmetric signature legality verification on the blockchain transaction

10. The method according to claim 9, wherein the routing device comprises a load-balancing device.

11. The method according to claim 8, wherein:

the second blockchain node further comprises a gateway; and

performing the asymmetric signature legality verification on the blockchain transaction comprises selecting, by the gateway, a server according to load balancing and performing, by the server, the asymmetric signature legality verification on the blockchain transaction.

12. The method according to claim 8, wherein performing the asymmetric signature legality verification on the blockchain transaction comprises:

obtaining a public key of a public-private key pair of a user, wherein the blockchain transaction is encrypted with a private key of the public-private key pair;

obtaining decrypted information of the blockchain transaction by decrypting the blockchain transaction with the public key; and

verifying the decrypted information of the blockchain transaction.

13. A non-transitory computer-readable storage medium storing instructions that, when

executed by one or more processors, cause the one or more processors to perform the method of any one of claims 1 to 12.

14. A system comprising one or more processors and one or more memories coupled to the one or more processors and configured with instructions executable by the one or more processors to cause the system to perform the method according to any one of claims 1 to 12.

15. A computer program product comprising program instructions, which when executed by one or more processors cause the one or more processors to perform a method according to any of claims 1 to 12.