## Claims

1. A method comprising:

before a consensus verification phase begins:

receiving, by a first blockchain node, a blockchain transaction from a client, wherein the first blockchain node comprises a plurality of servers and a memory coupled to the plurality of servers;

selecting, by the first blockchain node, a first server of the plurality of servers according to load balancing among the plurality of servers;

performing, by the first server, an asymmetric signature legality verification on the blockchain transaction;

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

storing, by the first blockchain node, the blockchain transaction into the memory; 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:

selecting, by the first blockchain node, a second server of the plurality of servers according to load balancing among the plurality of servers; and

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

2. The method according to claim 1, wherein the plurality of servers share one or more of the following: one node identity (ID) corresponding to the first blockchain node, a point-to-point routing table, and a pair of asymmetric public and private keys corresponding to the first blockchain node.

3. The method according to claim 1, wherein:

the first blockchain node further comprises a routing device coupled to the plurality of servers;

selecting, by the first blockchain node, the first server of the plurality of servers according to

load balancing among the plurality of servers comprises selecting, by the routing device, the first server of the plurality of servers according to load balancing among the plurality of servers; and

selecting, by the first blockchain node, the second server of the plurality of servers according to load balancing among the plurality of servers comprises selecting, by the routing device, the second server of the plurality of servers according to load balancing among the plurality of servers.

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

5. The method according to claim 1, wherein:

the first blockchain node further comprises a gateway;

selecting, by the first blockchain node, the first server of the plurality of servers according to load balancing among the plurality of servers comprises selecting, by the gateway, the first server of the plurality of servers according to load balancing among the plurality of servers; and

selecting, by the first blockchain node, the second server of the plurality of servers according to load balancing among the plurality of servers comprises selecting, by the gateway, the second server of the plurality of servers according to load balancing among the plurality of servers.

6. 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 associated with the client, 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.

7. 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.

8. The method according to claim 1, wherein:

before generating, by the first blockchain node, the pre-processed data block, further comprising transferring the plurality of blockchain transactions from the memory to a third server of the plurality of servers, 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 third server, the pre-processed data block.

9. A method comprising:

before a consensus verification phase begins:

selecting, by a second blockchain node, a first server from a plurality of servers according to load balancing among the plurality of servers, wherein the second blockchain node comprises the plurality of servers and a memory coupled to the plurality of servers;

receiving, by the first server, a blockchain transaction broadcast by a first blockchain node;

performing, by the first server, an asymmetric signature legality verification on the blockchain transaction;

in response to the first server determining that the blockchain transaction passes the asymmetric signature legality verification, storing, by the first server, the blockchain transaction into the memory; and

during the consensus verification phase:

selecting, by the second blockchain node, a second server from the plurality of servers according to load balancing among the plurality of servers;

receiving, by the second server, 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 server, consensus verification on the pre-processed data block.

10. The method according to claim 9, wherein the plurality of servers share one or more of the following: one node identity (ID) corresponding to the second blockchain node, a

point-to-point routing table, and a pair of asymmetric public and private keys corresponding to the second blockchain node.

11. The method according to claim 9, wherein:

the second blockchain node further comprises a routing device coupled to the plurality of servers;

selecting, by the second blockchain node, the first server from the plurality of servers according to load balancing among the plurality of servers comprises selecting, by the routing device, the first server from the plurality of servers according to load balancing among the plurality of servers; and

selecting, by the second blockchain node, the second server from the plurality of servers according to load balancing among the plurality of servers comprises selecting, by the routing device, the second server from the plurality of servers according to load balancing among the plurality of servers.

12. The method according to claim 11, wherein: the routing device comprises a load-balancing device.

13. The method according to claim 9, wherein:

the second blockchain node further comprises a gateway;

selecting, by the second blockchain node, the first server from the plurality of servers according to load balancing among the plurality of servers comprises selecting, by the gateway, the first server from the plurality of servers according to load balancing among the plurality of servers; and

selecting, by the second blockchain node, the second server from the plurality of servers according to load balancing among the plurality of servers comprises selecting, by the gateway, the second server from the plurality of servers according to load balancing among the plurality of servers.

14. The method according to claim 9, 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 associated with the blockchain transaction, 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.

15. A non-transitory computer-readable storage medium storing instructions that, when executed by one or more processors associated with one or more servers of a second blockchain node, cause the one or more processors to perform operations comprising:

before a consensus verification phase begins:

selecting, by the second blockchain node, a first server from a plurality of servers according to load balancing among the plurality of servers, wherein the second blockchain node comprises the plurality of servers and a memory coupled to the plurality of servers;

receiving, by the first server, a blockchain transaction broadcast by a first blockchain node;

performing, by the first server, an asymmetric signature legality verification on the blockchain transaction;

in response to the first server determining that the blockchain transaction passes the asymmetric signature legality verification, storing, the first server, the transaction request into the memory; and

during the consensus verification phase:

selecting, by the second blockchain node, a second server from the plurality of servers according to load balancing among the plurality of servers;

receiving, by the second server, 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 server, consensus verification on the pre-processed data block.

16. The non-transitory computer-readable storage medium according to claim 15, wherein the plurality of servers share one or more of the following: one node identity (ID) corresponding to the second blockchain node, a point-to-point routing table, and a pair of asymmetric public and private keys corresponding to the second blockchain node.

17. The non-transitory computer-readable storage medium according to claim 15, wherein:

the second blockchain node further comprises a routing device coupled to the plurality of

servers;

selecting, by the second blockchain node, the first server from the plurality of servers according to load balancing among the plurality of servers comprises selecting, by the routing device, the first server from the plurality of servers according to load balancing among the plurality of servers; and

selecting, by the second blockchain node, the second server from the plurality of servers according to load balancing among the plurality of servers comprises selecting, by the routing device, the second server from the plurality of servers according to load balancing among the plurality of servers.

18. The non-transitory computer-readable storage medium according to claim 17, wherein the routing device comprises a load-balancing device.

19. The non-transitory computer-readable storage medium according to claim 15, wherein:

the second blockchain node further comprises a gateway;

selecting, by the second blockchain node, the first server from the plurality of servers according to load balancing among the plurality of servers comprises selecting, by the gateway, the first server from the plurality of servers according to load balancing among the plurality of servers; and

selecting, by the second blockchain node, the second server from the plurality of servers according to load balancing among the plurality of servers comprises selecting, by the gateway, the second server from the plurality of servers according to load balancing among the plurality of servers.

20. The non-transitory computer-readable storage medium according to claim 15, 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 associated with blockchain transaction, 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.