CLAIMS:

1. A computer-implemented method for atomic broadcast, the method comprising:

transmitting, by a first blockchain computer node of a number (N) of blockchain computer nodes of a blockchain, data to each of a plurality of second blockchain computer nodes of the N blockchain computer nodes, wherein N is at least four;

obtaining, by the first blockchain computer node, at least (N-F) signatures certifying the data respectively, wherein the at least (N-F) signatures respectively correspond to at least (N-F) blockchain computer nodes among the first and second blockchain computer nodes, wherein F is a largest integer that is not greater than (N-1)/2;

generating, by the first blockchain computer node, a hash value of the data;

associating, by the first blockchain computer node, the hash value with the at least (N-F) signatures;

generating, by the first blockchain computer node, a blockchain transaction comprising the hash value, the at least (N−F) signatures, and a group identification corresponding to the N blockchain computer nodes; and

submitting, by the first blockchain computer node, the generated blockchain transaction to one or more blockchain computer nodes of the blockchain for adding into the blockchain based on a consensus verification of the generated blockchain transaction, wherein the group identification, when stored into the blockchain, identifies the N blockchain computer nodes.

2. The method of claim 1, wherein transmitting the data to each of the plurality of second blockchain computer nodes comprises:

encrypting the data with a plurality of public keys respectively corresponding to the plurality of second blockchain computer nodes to obtain a plurality of pieces of encrypted data; and

transmitting the plurality of pieces of encrypted data to the plurality of second blockchain computer nodes, respectively.

3. The method of claim 1, wherein the at least (N-F) signatures certifying the data comprises:

(N-F) signatures certifying receipt of the data and validity of the data.

4. The method of claim 1, wherein each of the (N-F) signatures comprises:

an encryption of the data with a private key corresponding to one of the at least (N-F) blockchain computer nodes.

5. The method of claim 1, wherein obtaining the at least (N-F) signatures comprises:

obtaining at least (N-F) consistent and valid signatures respectively from (N-F) distinct blockchain computer nodes of the N blockchain computer nodes.

6. The method of claim 1, wherein:

the at least (N-F) signatures are respectively obtained from the plurality of second blockchain computer nodes.

7. The method of claim 1, wherein:

one of the at least (N-F) signatures is obtained from the first blockchain computer node; and

the other at least (N-F-1) signatures are respectively obtained from the plurality of second blockchain computer nodes.

8. The method of claim 1, further comprising:

obtaining, by the first blockchain computer node, the blockchain transaction from the blockchain; and

verifying, by the first blockchain computer node, the data by verifying if a number of signatures comprised in the obtained blockchain transaction reaches (N-F).

9. The method of claim 1, further comprising:

locally executing, by the first blockchain computer node, the data according to an order of the blockchain transaction stored in the blockchain relative to other blockchain transactions stored in the blockchain.

10. The method of claim 9, further comprising:

receiving, by the first blockchain computer node, a synchronization request from a requesting blockchain computer node;

determining, by the first blockchain computer node, if the requesting blockchain computer node is one of the N blockchain computer nodes; and

in response to determining that the requesting blockchain computer node is one of the N blockchain computer nodes, transmitting, by the first blockchain computer node, the data to the requesting blockchain computer node via a non-blockchain computer network channel.

11. The method of claim 10, wherein:

the requesting blockchain computer node is one of F non-functioning blockchain computer nodes of the N blockchain computer nodes.

12. The method of claim 1, wherein:

the blockchain is a public blockchain; and

the data comprises one or more identifications of one or more senders of a private transaction, one or more identifications of one or more recipients of the private transaction, and one or more transaction amounts of the private transaction.

13. A non-transitory computer-readable storage medium of a first blockchain computer node, the non-transitory computer-readable storage medium storing instructions that, when executed by a processor, cause the processor to perform operations comprising:

transmitting data to each of a plurality of second blockchain computer nodes of a number (N) of blockchain computer nodes of a blockchain, wherein N is at least four;

obtaining at least (N-F) signatures certifying the data respectively, wherein the at least (N-F) signatures respectively correspond to at least (N-F) blockchain computer nodes among the first and second blockchain computer nodes, wherein F is a largest integer that is not greater than (N-1)/2;

generating a hash value of the data;

associating the hash value with the at least (N-F) signatures;

submitting the hash value and the at least (N-F) signatures in association with each other to one or more blockchain computer nodes of the blockchain for adding into the blockchain based on a consensus verification of the hash value and the at least (N-F) signatures;

locally executing the data according to an order of the blockchain transaction stored in the blockchain relative to other blockchain transactions stored in the blockchain;

receiving a synchronization request from a requesting blockchain computer node;

determining if the requesting blockchain computer node is one of the N blockchain computer nodes; and

in response to determining that the requesting blockchain computer node is one of the N blockchain computer nodes, transmitting the data to the requesting blockchain computer node via a non-blockchain computer network channel..

14. The non-transitory computer-readable storage medium of claim 13, wherein submitting the hash value and the at least (N-F) signatures to the one or more blockchain computer nodes of the blockchain comprises:

generating a blockchain transaction comprising the hash value and the at least (N-F) signatures; and

transmitting the blockchain transaction to the one or more blockchain computer nodes of the blockchain for adding into the blockchain.

15. The non-transitory computer-readable storage medium of claim 14, wherein the operations further comprise:

obtaining the blockchain transaction from the blockchain; and

verifying the data by verifying if a number of signatures comprised in the obtained blockchain transaction reaches (N-F).

16. A system acting as a first blockchain computer node, the system comprising one or more processors and one or more memories configured with instructions that, when executed by the one or more processors, cause the system to perform operations comprising:

transmitting data to each of a plurality of second blockchain computer nodes of a number (N) of blockchain computer nodes of a blockchain, wherein N is at least four;

obtaining at least (N-F) signatures certifying the data respectively, wherein the at least (N-F) signatures respectively correspond to at least (N-F) blockchain computer nodes among the first and second blockchain computer nodes, wherein F is a largest integer that is not greater than (N-1)/2;

generating a hash value of the data;

associating the hash value with the at least (N-F) signatures;

generating a blockchain transaction comprising the hash value, the at least (N−F) signatures, and a group identification corresponding to the N blockchain computer nodes; and

submitting the generated blockchain transaction to one or more blockchain computer nodes of the blockchain for adding into the blockchain based on a consensus verification of the generated blockchain transaction, wherein the group identification, when stored into the blockchain, identifies the N blockchain computer nodes.