CLAIMS

1. A method, comprising:

receiving, at a first node of a blockchain network, a first data fragment of proposed transaction data that is sent by a second node in a unicast mode, wherein a consensus algorithm of the blockchain network is a practical Byzantine fault tolerance (PBFT) algorithm, and wherein data fragments of the proposed transaction data that are sent by the second node in the unicast mode to nodes of the blockchain network are different from each another;

broadcasting, by the first node, the first data fragment to the nodes of the blockchain network;

receiving, at the first node, one or more second data fragments of the proposed transaction data that are broadcast by one or more nodes of the blockchain network;

determining, by the first node, whether a number of data fragments of the proposed transaction data that have been received by the first node, including the first data fragment and the one or more second data fragments, reaches an erasure code recovery threshold, wherein the erasure code recovery threshold is equal to or less than $2f+1$, wherein f represents a number of fault-tolerable nodes in the PBFT algorithm, and wherein f can be obtained based on an equation $N=3f+1$, wherein N represents a total number of the nodes of the blockchain network; and

in response to determining that the number of data fragments of the proposed transaction data that have been received by the first node reaches the erasure code recovery threshold, performing data recovery on the data fragments that have been received by the first node based, at least in part, on an erasure code reconstruction algorithm to obtain original content of the proposed transaction data.

2. The method according to claim 1, wherein the method further comprises:

determining whether a node of the blockchain network is elected as a primary node;

in response to determining that the node is elected as the primary node, fragmenting the proposed transaction data into a plurality of data fragments based, at least in part, on an erasure code algorithm; and

separately sending the data fragments to other nodes of the blockchain network in the unicast mode.

3. The method according to claim 1, wherein the receiving the first data fragment of the proposed transaction data that is sent by the second node in the unicast mode includes:

receiving a pre-prepare message sent by the second node in the unicast mode, wherein the pre-prepare message includes the first data fragment of the proposed transaction data.

4. The method according to claim 3, wherein the broadcasting the first data fragment to the nodes of the blockchain network comprises:

broadcasting a prepare message to the nodes of the blockchain network, wherein the prepare message includes the first data fragment.

5. The method according to claim 2, wherein the fragmenting the proposed transaction data into the plurality of data fragments based, at least in part, on the erasure code algorithm includes:

performing compression processing on the proposed transaction data based, at least in part, on a compression algorithm to obtain compressed transaction data; and

fragmenting the compressed transaction data into the plurality of data fragments based, at least in part, on the erasure code algorithm; and

wherein the performing data recovery on the data fragments that have been received by the first node based, at least in part, on the erasure code reconstruction algorithm to obtain the original content of the proposed transaction data includes:

performing data recovery on the data fragments that have been received by the first node based, at least in part, on the erasure code reconstruction algorithm to obtain the compressed transaction data; and

performing decompression processing on the compressed transaction data based, at least in part, on a decompression algorithm corresponding to the compression algorithm, to obtain the original content of the proposed transaction data.

6. The method according to claim 2, wherein the fragmenting the proposed transaction data into the plurality of data fragments based, at least in part, on the erasure code algorithm comprises:

performing encryption processing on the proposed transaction data based, at least in part, on an encryption algorithm and an encryption key to obtain encrypted transaction data; and

fragmenting the encrypted transaction data into the plurality of data fragments based, at least in part, on the erasure code algorithm; and

wherein the performing data recovery on the data fragments that have been received by the first node based, at least in part, on the erasure code reconstruction algorithm to obtain the original content of the proposed transaction data comprises:

performing data recovery on the data fragments that have been received by the first node based, at least in part, on the erasure code reconstruction algorithm to obtain the encrypted transaction data; and

performing decryption processing on the encrypted transaction data based, at least in part, on a decryption algorithm corresponding to the encryption algorithm and a decryption key corresponding to the encryption key, to obtain the original content of the proposed transaction data.

7. The method according to claim 6, wherein the encryption algorithm is a threshold encryption algorithm, the decryption algorithm is a threshold decryption algorithm corresponding to the threshold encryption algorithm, the decryption key is fragmented into a plurality of sub-keys, and each of the sub-keys is held by a respective node, and

wherein the performing decryption processing on the encrypted transaction data based, at least in part, on the decryption algorithm corresponding to the encryption algorithm and the decryption key corresponding to the encryption key comprises:

collecting sub-keys held by one or more node devices;

determining whether a number of collected sub-keys reaches a decryption threshold; and

in response to determining that the number of collected sub-keys reaches the decryption threshold, reconstructing the decryption key based, at least in part, on the collected sub-keys, and performing decryption processing on the encrypted transaction data based, at least in part, on the

threshold decryption algorithm corresponding to the threshold encryption algorithm and the decryption key.

8. The method according to claim 1, wherein the proposed transaction data is a transaction list constructed using to-be-negotiated transactions broadcast by user clients in a consensus period of the second node, and the proposed transaction data is fragmented into different data fragments in accordance with the total number of the nodes of the blockchain network.

9. The method according to claim 1, wherein the blockchain network is a consortium blockchain network.

10. An apparatus, comprising:

a receiving module, configured to receive a first data fragment of proposed transaction data that is sent by a first node of a blockchain network in a unicast mode, wherein a consensus algorithm of the blockchain network is a practical Byzantine fault tolerance (PBFT) algorithm, and wherein data fragments of the proposed transaction data that are sent by the first node to nodes of the blockchain network in the unicast mode are different from each another;

a sending module, configured to broadcast the first data fragment to the nodes of the blockchain network, and receive one or more data fragments of the proposed transaction data that are broadcast by one or more second nodes of the blockchain network;

a determining module, configured to determine whether a number of received data fragments of the proposed transaction data reaches an erasure code recovery threshold, wherein the erasure code recovery threshold is equal to or less than $2f+1$, wherein f represents a number of fault-tolerable nodes in the PBFT algorithm, and wherein f can be obtained based on an equation $N=3f+1$, wherein N represents a total number of the nodes of the blockchain network; and

a recovery module, configured to: in response to determining that the number of received data fragments of the proposed transaction data reaches the erasure code recovery threshold,

perform data recovery on the received data fragments based, at least in part, on an erasure code reconstruction algorithm to obtain original content of the proposed transaction data.

11. The apparatus according to claim 10, wherein the apparatus further comprises:

a fragmentation module, configured to determine whether a node of the blockchain network is elected as a primary node, and in response to determining that the node is elected as the primary node, fragment the proposed transaction data into a plurality of data fragments based, at least in part, on an erasure code algorithm; and

wherein the sending module is further configured to separately send the data fragments to other nodes of the blockchain network in the unicast mode.

12. The apparatus according to claim 10, wherein the receiving module is configured to:

receive a pre-prepare message sent by the first node in the unicast mode, wherein the pre-prepare message includes the first data fragment of the proposed transaction data.

13. The apparatus according to claim 12, wherein the sending module is configured to:

broadcast a prepare message to the nodes, wherein the prepare message includes the first data fragment.

14. The apparatus according to claim 11, wherein the fragmentation module is configured to:

perform compression processing on the proposed transaction data based, at least in part, on a compression algorithm to obtain compressed transaction data; and

fragment the compressed transaction data into the plurality of data fragments based, at least in part, on the erasure code algorithm; and

wherein the recovery module is configured to:

perform data recovery on the received data fragments based, at least in part, on the erasure code reconstruction algorithm to obtain the compressed transaction data; and

perform decompression processing on the compressed transaction data based, at least in part, on a decompression algorithm corresponding to the compression algorithm, to obtain the original content of the proposed transaction data.

15. The apparatus according to claim 11, wherein the fragmentation module is configured to:

perform encryption processing on the proposed transaction data based, at least in part, on an encryption algorithm and an encryption key to obtain encrypted transaction data; and

fragment the encrypted transaction data into the plurality of data fragments based, at least in part, on the erasure code algorithm; and

wherein the recovery module is configured to:

perform data recovery on the received data fragments based, at least in part, on the erasure code reconstruction algorithm to obtain the encrypted transaction data; and

perform decryption processing on the encrypted transaction data based, at least in part, on a decryption algorithm corresponding to the encryption algorithm and a decryption key corresponding to the encryption key, to obtain the original content of the proposed transaction data.

16. The apparatus according to claim 15, wherein the encryption algorithm is a threshold encryption algorithm, the decryption algorithm is a threshold decryption algorithm corresponding to the threshold encryption algorithm, the decryption key is fragmented into a plurality of sub-keys, and each of the sub-keys is held by a respective node; and

wherein the recovery module is further configured to:

collect sub-keys held by one or more nodes;

determine whether a number of collected sub-keys reaches a decryption threshold; and

in response to determining that the number of collected sub-keys reaches the decryption threshold, reconstruct the decryption key based, at least in part, on the collected sub-keys, and perform decryption processing on the encrypted transaction data based, at least in part,

on the threshold decryption algorithm corresponding to the threshold encryption algorithm and the decryption key.

17. The apparatus according to claim 10, wherein the proposed transaction data is a transaction list constructed using to-be-negotiated transactions broadcast by user clients in a consensus period of the first node, and the proposed transaction data is fragmented into different data fragments in accordance with the total number of the nodes of the blockchain network.

18. The apparatus according to claim 10, wherein the blockchain network is a consortium blockchain network.

19. An electronic device, comprising:

one or more processors; and

a memory, configured to store machine-executable instructions, wherein

by reading and executing the machine-executable instructions stored in the memory, the one or more processors are configured to:

receive a data fragment of transaction data that is sent by a node of a blockchain network in a unicast mode, wherein a consensus algorithm of the blockchain network is a practical Byzantine fault tolerance (PBFT) algorithm, wherein the node fragments the proposed transaction data into a plurality of data fragments including the data fragment, and wherein respective data fragments of the transaction data that are sent by the node to nodes of the blockchain network in the unicast mode are different from one another;

broadcast the data fragment to the nodes in the blockchain network;

receive one or more other data fragments of the transaction data that are broadcast by one or more nodes in the blockchain;

determine whether a number of received data fragments of the transaction data reaches an erasure code recovery threshold, wherein the erasure code recovery threshold is equal to or less than $2f+1$, wherein f represents a number of fault-tolerable nodes in the PBFT algorithm, and wherein f can be obtained based on an equation $N=3f+1$, wherein N represents a total number of the nodes in the blockchain network; and

in response to determining that the number of received data fragments of the transaction data reaches the erasure code recovery threshold, perform data recovery on the received data fragments based, at least in part, on an erasure code reconstruction algorithm to obtain original content of the transaction data.

20. The electronic device according to claim 19, wherein the blockchain network is a consortium blockchain network.