CLAIMS

1. A transaction consensus processing method for a blockchain, the blockchain including a plurality of nodes, wherein a target node of the plurality of nodes that initiates a proposition performs compression processing on proposed transaction data based on a predetermined compression algorithm, and fragments the compressed transaction data into a number of data fragments based on an erasure code algorithm, and wherein a consensus algorithm of the blockchain is a practical Byzantine fault tolerance, PBFT, algorithm, the method comprising:

receiving (102), by a node of the plurality of nodes, a data fragment of the number of data fragments of the transaction data that is sent by the target node in a unicast mode, including:

receiving, by the node, a pre-prepare message sent by the target node in the unicast mode, wherein the pre-prepare message includes the data fragment of the transaction data; and

obtaining and storing, by the node, the data fragment included in the pre-prepare message, wherein the pre-prepare message sent by the target node to the node and each pre-prepare message sent by the target node to other nodes of the plurality of nodes include different data fragments of the transaction data;

broadcasting (104), by the node, the received data fragment to the other nodes of the plurality of nodes in the blockchain, and receiving, by the node, further data fragments of the transaction data that are broadcast by the other nodes; determining (106), by the node, whether a number of received data fragments of the transaction data, including the data fragment received (102) from the target node and the further data fragments received from the other nodes, reaches an erasure code recovery threshold of an erasure code reconstruction algorithm; and

in response to determining (106) that the number of received data fragments of

the transaction data reaches the erasure code recovery threshold, performing (108), by the node, data recovery on the received data fragments based on the erasure code reconstruction algorithm to recover the transaction data, performing, by the node, decompression processing on the recovered transaction data based on a decompression algorithm corresponding to the compression algorithm to obtain original content of the transaction data, and completing, by the node, consensus processing on the obtained original content of the transaction data.

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

generating, by the node, transaction data proposed by a further node of the plurality of nodes;

performing, by the node, compression processing on the transaction data proposed by the further node based on the predetermined compression algorithm, and fragmenting the compressed transaction data into a number of data fragments based on the erasure code algorithm; and

sending, by the node, the number of data fragments to the other nodes separately in the unicast mode.

3. The method according to claim 1, wherein the broadcasting (104) the received data fragment to the other nodes in the blockchain includes:

broadcasting a prepare message to the other nodes in the blockchain, wherein the prepare message includes the obtained data fragment, so that upon receiving the prepare message, the other nodes obtain and store the data fragment in the prepare message.

4. The method according to claim 1 or 2, wherein the fragmenting the proposed transaction data into the number of data fragments based on the erasure code algorithm includes:

performing encryption processing on the proposed transaction data based on a predetermined encryption algorithm and an encryption key; and

fragmenting the encrypted transaction data into the number of data fragments based on the erasure code algorithm; and

the performing data recovery on the received data fragment based on the erasure code reconstruction algorithm includes:

performing data recovery on the received data fragment based on the erasure code reconstruction algorithm; and

obtaining the original content of the transaction data by performing decryption processing on recovered transaction data based on a decryption algorithm corresponding to the encryption algorithm and a decryption key corresponding to the encryption key.

5. The method according to claim 4, 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 number of sub-keys, and the sub-keys are held by nodes respectively; and

the performing decryption processing on the recovered transaction data based on the decryption algorithm corresponding to the encryption algorithm and the decryption key corresponding to the encryption key includes:

collecting sub-keys held by other nodes;

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

in response to determining that the number of collected sub-keys reaches the predetermined decryption threshold, reconstructing the decryption key based on the collected sub-keys, and performing decryption processing on the recovered transaction data based on the threshold decryption algorithm corresponding to the threshold encryption algorithm and the decryption key.

6. The method according to claim 1, wherein the transaction data proposed by the target node is a transaction list, and the number is a total number of nodes in the blockchain.

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

8. An electronic device, comprising:

a processor; and

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

by reading and executing the machine-executable instructions stored in the memory and corresponds to control logic of transaction consensus processing for a blockchain, the processor is configured to perform a method according to any one of the preceding claims.