CLAIMS

1. A method for processing transaction consensus in a blockchain network, wherein the blockchain network include at least one primary node device and a plurality of secondary node devices and wherein a primary node device fragments proposed transaction data into a specified number of data fragments based on an erasure code algorithm, the method comprising:

receiving (102) a data fragment of the transaction data that is sent by the primary node device in a unicast mode, wherein respective data fragments sent by the primary node device in the unicast mode to individual node devices are different from one another;

broadcasting (104) the received data fragment to other node devices in the blockchain network, and receiving data fragments of the transaction data that are broadcast by the other node devices;

determining (106) whether the number of received data fragments of the transaction data reaches an erasure code recovery threshold; and

in response to determining that the number of received data fragments of the transaction data reaches the erasure code recovery threshold, performing (108) data recovery on the received data fragments based on an erasure code reconstruction algorithm to obtain original content of the transaction data, to complete consensus processing with respect to the original content of the transaction data,

wherein the performing data recovery on the received data fragments based on the erasure code reconstruction algorithm to obtain the original content of the transaction data includes:

performing data recovery on the received data fragments based on the erasure code reconstruction algorithm, to obtain transaction data compressed by the primary node device based on a predetermined compression algorithm; and

performing decompression processing on the recovered transaction data based on a decompression algorithm corresponding to the predetermined compression algorithm of the primary node device, to obtain the original content of the transaction data.

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

determining whether a current node device is elected as the primary node device;

in response to determining that the current node device is elected as the primary node device, fragmenting the proposed transaction data into the specified number of data fragments based on the erasure code algorithm; and

separately sending the specified number of data fragments to each of the other node devices in a unicast mode.

3. The method according to claim 1, wherein a consensus algorithm equipped on the blockchain is a practical Byzantine fault tolerance, PBFT, algorithm; and wherein the receiving the data fragment of the transaction data that is sent by the primary node device in a unicast mode includes:

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

obtaining and storing the data fragment included in the pre-prepare message.

4. The method according to claim 3, wherein the broadcasting the received data fragment to the other node devices in the blockchain network comprises:

broadcasting a prepare message to the other node devices in the blockchain network, wherein the prepare message includes the received data fragment, so that when receiving the prepare message, the other node devices obtain and store the data fragment included in the prepare message.

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

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 specified number of data fragments based on the erasure code algorithm; and

wherein the performing data recovery on the received data fragments based on the erasure code reconstruction algorithm to obtain the original content of the transaction data includes:

performing data recovery on the received data fragments based on the erasure code reconstruction algorithm, to obtain the encrypted transaction data; and

performing decryption processing on the recovered transaction data based 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 transaction data.

6. The method according to claim 5, 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 specified number of sub-keys, and each of the sub-keys is held by a respective node device, and

wherein 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 the other node devices;

determining whether the 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.

7. The method according to claim 1, wherein the transaction data proposed by the primary node device is a transaction list constructed using to-be-negotiated transactions broadcast by user clients in a current consensus period of the primary node device, and the specified number is a total number of node devices in the blockchain network.

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

9. 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 corresponding to control logic of processing transaction consensus in a blockchain network, the processor is configured to perform a method according to any one of the preceding claims.