

CLAIMS

What is claimed is:

1. A method for blockchain data processing, the method comprising:
 - receiving blockchain transaction data of a plurality of transaction participants, each of the plurality of transaction participants providing a respective certificate indicating a respective legal membership in a blockchain network, the respective legal membership enabling processing of the blockchain transaction data;
 - performing a mutual identity query to confirm whether each of the plurality of transaction participants have the respective legal membership in the blockchain network;
 - determining supervision keys of a supervision node in the blockchain network, wherein the supervision node corresponds to a supervisor and the supervision keys are dynamically updated based on a predetermined rule;
 - encrypting the blockchain transaction data by using the supervision keys; and
 - storing the blockchain transaction data.
2. The method according to claim 1, wherein the supervision keys comprise a supervision public key and a supervision private key that are generated based on an asymmetric encryption algorithm.
3. The method according to claim 2, wherein the asymmetric encryption algorithm comprises one of a Rivest–Shamir–Adleman algorithm, an Elgamal algorithm, a knapsack algorithm, a Rabin algorithm, Diffie–Hellman key exchange algorithm, and an elliptic curve cryptographic algorithm.
4. The method according to claim 2, wherein in response to determining that the supervision public key is updated, a blockchain node receives and records a new supervision public key after the supervision node broadcasts the new supervision public key in the blockchain network.
5. The method according to claim 4, wherein determining the supervision keys of the supervision node in the blockchain network comprises:

receiving the new supervision public key broadcasted by the supervision node in the blockchain network; and

updating a locally stored supervision key to the new supervision public key.

6. The method according to claim 4, wherein determining the supervision keys of the supervision node in the blockchain network comprises:

receiving the new supervision public key broadcasted by the supervision node in the blockchain network, wherein the new supervision public key comprises data signed by using a non-updated supervision private key;

performing a signature verification on the signed data by using a public key of stored previously-updated supervision keys; and

updating a locally stored supervision key to the new supervision public key in response to determining that the verification succeeds.

7. The method according to claim 2, wherein encrypting the blockchain transaction data by using the supervision keys comprises at least one of:

encrypting transaction content by using the supervision public key;

encrypting, by using the supervision public key, a private key used by a transaction participant to sign a transaction; or

encrypting, by using the supervision public key, a private key used by the transaction participant to sign a temporary identity.

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

receiving a supervision message sent by the supervisor; and

performing verification on the received supervision message by using the stored supervision public key.

9. The method according to claim 8, wherein the supervision message comprises data signed by the supervision node by using the supervision private key.

10. The method according to claim 1, wherein the blockchain network comprises a consortium blockchain.
11. The method according to claim 1, wherein the supervisor is included in the plurality of transaction participants and is determined based on an agreement of a majority of the plurality of transaction participants.
12. A device for blockchain data processing, the device comprising a plurality of modules configured to perform the method of any one of claims 1 to 11.