

CLAIMS

What is claimed is:

1. A method for blockchain data processing, the method comprising:
 - receiving, by a first blockchain node of a blockchain network, from a supervision node of the blockchain network, a new supervision public key;
 - updating, by the first blockchain node, a locally-stored non-updated supervision public key to the new supervision public key;
 - receiving, by the first blockchain node, blockchain transaction data of a plurality of transaction participants, wherein the blockchain transaction data corresponds to a transaction;
 - encrypting, by the first blockchain node, the blockchain transaction data using the new supervision public key;
 - storing, by the first blockchain node, the blockchain transaction data encrypted with the new supervision public key to a blockchain of the blockchain network; and
 - receiving a supervision message sent by the supervision node, wherein the supervision message comprises data signed by the supervision node using a new supervision private key paired with the new supervision public key, and wherein the supervision message is sent subsequent to the supervision node putting at least one transaction participant in a blacklist or preventing the transaction,
 - wherein the supervision node is configured to:
 - obtain the blockchain transaction data encrypted with the new supervision public key from the blockchain,
 - decrypt the blockchain transaction data using the new supervision private key,
 - perform transaction supervision on the transaction, and
 - initiate the supervision message responsive to the transaction supervision.
2. The method according to claim 1, wherein the new supervision public key and the new supervision private key 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 1, wherein the new supervision public key received by the first blockchain node is signed by a non-updated supervision private key that is paired with the locally-stored non-updated supervision public key, and wherein updating the locally-stored non-updated supervision public key comprises:

performing signature verification on the new supervision public key signed by the non-updated supervision private key by using the locally-stored non-updated supervision public key; and

updating the locally-stored non-updated supervision public key to the new supervision public key in response to determining that the signature verification succeeds.

5. The method according to claim 1, wherein encrypting the blockchain transaction data using the new supervision public key comprises at least one of:

encrypting transaction content using the new supervision public key;

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

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

6. The method according to claim 1, comprising:

performing, by the first blockchain node, verification on the received supervision message by the new supervision public key.

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

8. The method according to claim 1, wherein the supervision node is included in the plurality of transaction participants and is determined based on an agreement of a majority of the plurality of transaction participants.

9. 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 8.