Claims

1. A method for processing blockchain data, the method comprising:

receiving a registration of a transaction participant in a blockchain by using a blockchain registration authority;

performing an identity query to confirm that the transaction participant is an authorized user in the blockchain;

determining (602) a temporary identity information of the transaction participant in the blockchain;

performing (604) an identity signature for a transaction by using the temporary identity information, to generate blockchain data of the transaction participant; and

storing (606) the blockchain data in the blockchain,

wherein the temporary identity information is updated based on a predetermined replacement cycle.

2. The method according to claim 1, wherein the temporary identity information comprises data information generated based on a real identity information of the transaction participant.

3. The method according to claim 1, wherein the temporary identity information is processed based on an asymmetric encryption algorithm.

4. The method according to claim 3, 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.

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

sending a public key of the transaction participant to a specified other transaction participant.

6. The method according to claim 5, wherein performing the identity signature for the transaction by using the temporary identity information comprises:

performing the identity signature for the transaction by using a private key of the transaction participant.

7. The method according to claim 6, wherein the method further comprises:

encrypting the private key of the transaction participant by using the public key in regulation keys corresponding to a regulator; and

transmitting the encrypted private key to the regulator.

8. The method according to claim 5, wherein sending the public key of the transaction participant to the specified other transaction participant comprises:

transmitting data by using an end-to-end encryption channel.

9. The method according to claim 8, wherein the public key is generated by the end-to-end encryption channel based on a secure sockets layer protocol.

10. The method according to claim 1, wherein the temporary identity information is updated based on at least one of different transaction participants or different transactions.

11. The method according to claim 1, wherein the temporary identity information is configured to remove association between transactions.

12. An apparatus for processing blockchain data, the apparatus comprising plurality of modules configured to perform the method of any one of claims 1 to 11.