

CLAIMS

1. A blockchain-based privacy transaction method, applied to a node device of a trusted user, wherein the trusted user belongs to a plurality of trusted users selected and set by a blockchain user of a blockchain based on trust of the blockchain user to the plurality of trusted users, the trusted user is selected by the blockchain user from the plurality of trusted users and a trust setting transaction stored in a distributed database of the blockchain comprises identifiers of all trusted users of the plurality of trusted users, wherein the identifiers of all the trusted users of the plurality of trusted users uniquely determine information about all the trusted users of the plurality of trusted users and the method comprises:
- receiving (102) a first message sent by the blockchain user, wherein the first message comprises privacy-unprotected first data information;
 - converting (104) the privacy-unprotected first data information into privacy-protected second data information;
 - storing (106) the privacy-unprotected first data information in a local database of the node device of the trusted user;
 - sending (108) a second transaction to the blockchain, wherein the second transaction comprises the privacy-protected second data information, so that the second transaction is recorded in the distributed database of the blockchain after being verified;
 - obtaining (202) the trust setting transaction from the distributed database of the blockchain;
 - determining (204) other trusted users trusted by the blockchain user based on the trust setting transaction; and
 - transmitting (206), in an off-chain method, the privacy-unprotected first data information and the privacy-protected second data information to node devices of the other trusted users so that the privacy-unprotected first data information is stored in local databases of the node devices of the other trusted users after it is verified that the privacy-unprotected first data information is converted from the privacy-protected second data information.
2. The method according to claim 1, wherein the first message comprises a first digital signature made by the blockchain user at least for the privacy-unprotected first data information; and
- the method further comprises:

verifying the first message based on a predetermined verification rule so as to store the privacy-unprotected first data information in the local database of the node device of the trusted user after the verification succeeds, wherein the predetermined verification rule further comprises verifying that the first digital signature is made by the blockchain user at least for the privacy-unprotected first data information.

3. The method according to claim 2, wherein the second transaction further comprises a second digital signature made by the trusted user at least for the privacy-protected second data information and the first digital signature made by the blockchain user at least for the privacy-unprotected first data information.

4. The method according to any one of claims 1 to 3, further comprising:
receiving digital signatures made by the other trusted users at least based on the privacy-protected second data information; wherein
the second transaction further comprises the digital signature made by the other trusted users at least based on the privacy-protected second data information.

5. The method according to claim 1, wherein the privacy-protected second data information is a data digest of the privacy-unprotected first data information.

6. The method according to claim 1, wherein the first message comprises a transfer amount of the blockchain user to another blockchain user, the second transaction comprises the privacy-protected transfer amount and privacy-protected account balances of the blockchain user and the another blockchain user and the trusted user is also a trusted user corresponding to the another blockchain user in the trust setting transaction.

7. A computer device implementing a node device of a blockchain and configured to carry out the method according to any of the preceding claims.

8. One or more computer-readable storage media storing a computer program which, when run by a processor of a computer device, causes the processor to perform the method according to any one of claims 1 to 6.