

that the second data information included in the second transaction is originally generated by the node device of the blockchain user, the second transaction can further include the first digital signature that is included in the first message and that is made by the blockchain user at least for the privacy-unprotected first data information. Correspondingly, verification of the second transaction by the node device on the blockchain should include at least verification of the second digital signature based on the public key of the trusted user, so as to record the second transaction in the distributed database of the blockchain after the verification succeeds.

10 **[0042]** The blockchain user can set a plurality of trusted users when setting the trusted user. The blockchain user can select a trusted user from the plurality of trusted users and send the first message to the trusted user. Correspondingly, in addition to completing the blockchain-based privacy transaction method described in steps 102 to 108 in the previous embodiments, the trusted user should further transmit the first message sent by the blockchain user to node devices of other trusted users, so that the other trusted users store the privacy-unprotected first data information included in the first message in local databases of the node devices of the other trusted users. Specifically, as shown in FIG. 2, the step of transmitting the first message sent by the blockchain user to the node devices of other trusted users can include the following steps:

20 **[0043]** Step 202: Obtain the trust setting transaction from the distributed database of the blockchain.

[0044] Step 204: Determine other trusted users trusted by the blockchain user based on the trust setting transaction.

25 **[0045]** Step 206: Transmit, using an off-chain method, the privacy-unprotected first data information and the privacy-protected second data information to the node devices of the other trusted users trusted by the user, so that the first data information is stored in the local databases of the node devices of the other trusted users after it is verified that the second data information is converted from the first data information.

30 **[0046]** As described in the previous embodiments, the trust setting transaction includes identifiers of all trusted users determined by the blockchain user, such as account addresses of the trusted users, public keys of the trusted users, or account names of the trusted users that can uniquely determine information about the trusted

a receiving unit 502, configured to receive a first message sent by the blockchain user, where the first message includes privacy-unprotected first data information;
a conversion unit 504, configured to convert the privacy-unprotected first data information into privacy-protected second data information;
5 a storage unit 506, configured to store the first data information in a local database of the node device of the trusted user; and
a sending unit 508, configured to send a second transaction to the blockchain, where the second transaction includes the second data information, so that the second transaction is recorded in the distributed database of the blockchain after being
10 verified.

[0081] In other implementations, the first message includes a first digital signature made by the blockchain user at least for the privacy-unprotected first data information.

[0082] The apparatus 50 further includes a verification unit 510, configured to
15 verify the first message based on a predetermined verification rule so as to store the first data information in the local database of the node device of the trusted user after the verification succeeds, where the predetermined verification rule further includes verifying that the first digital signature is made by the blockchain user at least for the privacy-unprotected first data information.

20 **[0083]** In other implementations, the second transaction further includes 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.

[0084] In other shown implementations, the apparatus 50 further includes:
25 an obtaining unit 512, configured to obtain the trust setting transaction from the distributed database of the blockchain;
a determining unit 514, configured to determine other trusted users trusted by the blockchain user based on the trust setting transaction; and
a transmission unit 516, configured to transmit, in an off-chain method, the
30 privacy-unprotected first data information and the privacy-protected second data information to node devices of the other trusted users trusted by the blockchain user, so that the first data information is stored in the local databases of the node devices of the other trusted users after it is verified that the second data information is converted from the first data information.

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-protected second data information is converted from the privacy-unprotected first 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.

- 5 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.
- 10 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.
- 15
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.
- 20 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.
- 25 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.
- 30 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.