

CLAIMS

~~What is claimed is:~~

1. ____ A blockchain-based privacy transaction method, applied to a node device of a trusted
5 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 ~~determined by~~ selected by the blockchain user from the plurality of
trusted users and a trust setting transaction stored in a distributed database of the blockchain;
~~and the trust setting transaction~~ comprises identifiers of all trusted users ~~corresponding to a~~
10 ~~blockchain user;~~ 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;

15 converting (104) the privacy-unprotected first data information into privacy-protected
second data information;

storing ~~the~~ (106) the privacy-unprotected first data information in a local database of the
node device of the trusted user; ~~and~~

sending (108) a second transaction to the blockchain, wherein the second transaction
20 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
25 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
30 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:

~~obtaining the trust setting transaction from the distributed database of the blockchain; and
determining another trusted user trusted by the user based on the trust setting transaction;
and~~

~~transmitting, in an off chain method, the privacy unprotected first data information and the privacy protected second data information to a node device of the another trusted user trusted by the user, so that the first data information is stored in a local database of the node device of the another trusted user after it is verified that the first data information is converted from the second data information.~~

~~5. The method according to claim 4, further comprising:~~

receiving a digital ~~signatures~~signatures made by the ~~another~~other trusted ~~user~~users at least based on the privacy-protected second data information; wherein
the second transaction further comprises the digital signature made by the ~~another~~other trusted ~~user~~users at least based on the privacy-protected second data information.

~~6.~~

~~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.

~~7.~~

~~6.~~ The method according to claim 1, wherein the first message comprises a transfer amount of the blockchain user to another blockchain user, ~~and~~ 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.

5 ~~8. A blockchain-based privacy transaction application method, comprising:~~

~~obtaining a second transaction sent by~~

10 ~~7. A computer device implementing a node device of a trusted user from a distributed database of the blockchain, wherein the second transaction comprises privacy-protected second data information, the trusted user is determined by a trust-setting transaction stored in the distributed database of the blockchain, blockchain and the trust-setting transaction comprises identifiers of all trusted users corresponding to a blockchain user;~~

~~receiving privacy-unprotected first data information sent by the node device of the trusted user, wherein the first data information is stored in a local database of the node device of the trusted user; and~~

15 ~~verifying whether the privacy-protected second data information is converted from the privacy-unprotected first data information, and if yes, executing application logic on the second transaction.~~

20 ~~9. A blockchain-based privacy transaction apparatus, applied to a node device of a trusted user, wherein the trusted user is determined by a trust setting transaction stored in a distributed database of the blockchain, and the trust setting transaction comprises identifiers of all trusted users corresponding to a blockchain user; and the apparatus comprises:~~

~~a receiving unit, configured to receive a first message sent by the blockchain user, wherein the first message comprises privacy-unprotected first data information;~~

25 ~~a conversion unit, configured to convert the privacy-unprotected first data information into privacy-protected second data information;~~

~~a storage unit, configured to store the first data information in a local database of the node device of the trusted user; and~~

30 ~~a sending unit, configured to send a second transaction to the blockchain, wherein the second transaction comprises the second data information, so that the second transaction is recorded in the distributed database of the blockchain after being verified.~~

10. The apparatus according to claim 9, 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 apparatus further comprises a verification unit, configured to 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, 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.

11. The apparatus according to claim 10, 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.

12. The apparatus carry out the method according to any one of the preceding claims 9 to 11, further comprising:

an obtaining unit, configured to obtain the trust setting transaction from the distributed database of the blockchain;

a determining unit, configured to determine another trusted user trusted by the user based on the trust setting transaction; and

a transmission unit, configured to transmit, in an off chain method, the privacy unprotected first data information and the privacy protected second data information to a node device of the another trusted user trusted by the user, so that the first data information is stored in a local database of the node device of the another trusted user after it is verified that the first data information is converted from the second data information.

13. The apparatus according to claim 12, wherein

the receiving unit is configured to receive a digital signature made by the another trusted user at least based on the second data information; and

the second transaction further comprises the digital signature made by the another trusted user at least based on the second data information.

14. The apparatus according to claim 9, wherein the privacy protected second data information is a data digest of the privacy unprotected first data information.

~~15. The apparatus according to claim 9, wherein the first message comprises a transfer amount of the blockchain user to another blockchain user, and the second transaction comprises the privacy protected transfer amount and privacy protected account balances of the blockchain user and the another blockchain user; and~~

5 ~~the trusted user is also a trusted user corresponding to the another blockchain user in the trust setting transaction.~~

~~16. A blockchain-based privacy transaction application apparatus, comprising:~~

10 ~~an obtaining unit, configured to obtain a second transaction sent by a node device of a trusted user from a distributed database of the blockchain, wherein the second transaction comprises privacy protected second data information, the trusted user is determined by a trust setting transaction stored in the distributed database of the blockchain, and the trust setting transaction comprises identifiers of all trusted users corresponding to a blockchain user;~~

15 ~~a receiving unit, configured to receive privacy unprotected first data information sent by the node device of the trusted user, wherein the first data information is stored in a local database of the node device of the trusted user;~~

~~a verification unit, configured to verify whether the privacy protected second data information is converted from the privacy unprotected first data information; and~~

~~an application unit, configured to execute application logic on the second transaction.~~

~~17. A computer device, comprising a memory and a processor, wherein the memory stores~~

20 ~~8. One or more computer-readable storage media storing a computer program that can be which, when run by the processor, and of a computer device, causes the processor performsto perform the method according to any one of claims 1 to 7 when running the computer program.~~

25 ~~18. A computer device, comprising a memory and a processor, wherein the memory stores a computer program that can be run by the processor, and the processor performs the method according to claim 8 when running the computer program.~~

6.