

CLAIMS:

1. A computer-implemented method for implementing blockchain-based private transactions, wherein the method is performed by a first blockchain node to a private transaction, the method comprising:

receiving a request for executing a private transaction among at least some of a first plurality of members, wherein the request identifies the at least some of the first plurality of members, the request comprises the private transaction, and the private transaction corresponds to a pre-configured threshold;

determining, based on the request, a transaction group of the first plurality of member, wherein the transaction group is stored in a public blockchain;

determining a plurality of second blockchain nodes to the private transaction according to a blockchain contract in the public blockchain, wherein the plurality of second blockchain nodes include blockchain nodes of the at least some of the first plurality of members;

transmitting, via a non-blockchain computer network, transaction information to the plurality of second blockchain nodes, the transaction information comprising one or more senders of the private transaction, one or more recipients of the private transaction, and one or more transaction amounts of the private transaction;

obtaining a signature from each of a number of the plurality of second blockchain nodes certifying receipt of the transaction information; and

in response to obtaining the number of the signatures over the pre-configured threshold, storing at least a representation of the private transaction and the signatures in the public blockchain.

2. The method of claim 1, wherein:

the blockchain contract comprises an address of each of the first and second blockchain nodes to the private transaction; and

determining the plurality of second blockchain nodes to the private transaction according to the blockchain contract in the public blockchain comprises: determining the plurality of second blockchain nodes to the private transaction according to the address of each of the plurality of second blockchain nodes to the private transaction.

3. The method of claim 2, wherein:

the address of each of the first and second blockchain nodes comprises at least one of: an Internet Protocol (IP) address or a communication port number.

4. The method of any of claims 2 and 3, wherein:

the blockchain contract further comprises a public key associated with each of the first and second blockchain nodes to the private transaction; and

transmitting the transaction information to the plurality of second blockchain nodes comprises:

for each of the plurality of second blockchain nodes, encrypting the transaction information with the corresponding public key; and

transmitting the encrypted transaction information to each of the plurality of second blockchain nodes according to the address of each of the plurality of second blockchain nodes.

5. The method of any preceding claim, wherein:

the blockchain contract further comprises an identification of a group comprising each of the first and second blockchain nodes to the private transaction for notifying each of the first and second blockchain nodes of an involvement in the private transaction.

6. The method of any preceding claim, wherein the signature from each of the number of the plurality of second blockchain nodes certifying receipt of the transaction information comprises:

a hash value of the transaction information encrypted with a private key associated with each of the number of the plurality of second blockchain nodes.

7. The method of any preceding claim, further comprising:

executing the private transaction locally.

8. The method of any preceding claim, further comprising:

obtaining a request for the transaction information from one of the plurality of second blockchain nodes that has verified the number of signatures and has not received the transaction information; and

transmitting the transaction information to the one second blockchain node for the one second blockchain node to execute the private transaction locally.

9. The method of any preceding claim, wherein before determining the plurality of second blockchain nodes to the private transaction according to the blockchain contract in the public blockchain, further comprising:

storing blockchain node information in the public blockchain, the blockchain node information comprising a public key of each of the first and second blockchain nodes to the private transaction and an address of each of the first and second blockchain nodes.

10. The method of claim 9, wherein storing the blockchain node information in the public blockchain comprises:

transmitting a first blockchain transaction comprising the blockchain contract to one or more blockchain nodes of the public blockchain for deploying the blockchain contract in the public blockchain; and

transmitting one or more second blockchain transactions to one or more blockchain nodes of the public blockchain for invoking the deployed blockchain contract to store the blockchain node information in the deployed blockchain contract.

11. The method of any of claims 9 and 10, wherein:

the deployed blockchain contract is configured to bar changes to each of the first and second blockchain nodes to the private transaction after the blockchain node information is stored in the deployed blockchain contract.

12. The method of any preceding claim, wherein storing at least the representation of the private transaction and the signatures in the public blockchain comprises:

transmitting a third blockchain transaction comprising a transaction hash of the private transaction and the signatures to one or more blockchain nodes of the public blockchain for packing into the public blockchain, wherein the transaction hash is a hash value of at least the transaction information.

13. The method of any preceding claim, wherein, in response to obtaining the number of the signatures over the pre-configured threshold, storing at least the representation of the private transaction and the signatures in the public blockchain comprises:

in response to respectively obtaining signatures of all of the second blockchain nodes to the private transaction, storing at least the representation of the private transaction and the signatures in the public blockchain.

14. A system for implementing blockchain-based private transactions, comprising:
one or more processors; and
one or more computer-readable memories coupled to the one or more processors and having instructions stored thereon that are executable by the one or more processors to perform the method of any of claims 1 to 13.

15. An apparatus for implementing blockchain-based private transactions, comprising a plurality of modules for performing the method of any of claims 1 to 13.

16. A non-transitory computer-readable medium having stored therein instructions that, when executed by a processor of a device, cause the device to perform the method of any of claims 1 to 13.