WHAT IS CLAIMED IS:

1. A computer-implemented method of a client node participating in a blockchain confidential transaction, the method comprising:

obtaining a secret key, by a client node, according to a threshold secret sharing scheme agreed to by a plurality of client nodes;

generating one or more commitment values of a blockchain confidential transaction of the client node by applying a cryptographic commitment scheme to transaction data, wherein the one or more commitment values comprise:

a first commitment value generated based on a pre-transaction account balance of the client node;

a second commitment value generated based on a transaction amount of the blockchain confidential transaction; and

a third commitment value generated based on the first commitment value and the second commitment value and corresponding to a post-transaction account balance of the client node;

generating encrypted transaction information of the blockchain confidential transaction by encrypting the transaction data using the secret key; and

transmitting, to a consensus node of a blockchain network, a content of the blockchain confidential transaction for execution, wherein the content of the blockchain confidential transaction comprises:

the one or more commitment values;

the encrypted transaction information; and

one or more zero-knowledge proofs of the transaction data;

retrieving, by the client node and from the consensus node, the encrypted transaction information;

determining, by the client node, that the secret key is no longer present in a local data storage of the client node;

determining, by the client node, that the client node does not have access to the secret key in response to determining that the secret key is no longer present in the local data storage of the client node;

in response to determining that the client node does not have access to the secret key, communicating, by the client node, with at least the threshold number of other client nodes over a non-blockchain network;

obtaining, by the client node, at least a threshold number of parts of the secret key from at least the threshold number of other client nodes over the non-blockchain network;

recovering, by the client node, the secret key using at least the threshold number of parts of the secret key according to the threshold secret sharing scheme; and

decrypting, by the client node, the encrypted transaction information using the recovered secret key.

2. The method of claim 1, wherein the transaction data of the blockchain confidential transaction comprises one or both of an account balance of the client node before the blockchain confidential transaction or a transaction amount of the blockchain confidential transaction.

3. The method of claim 1, wherein the one or more zero-knowledge proofs of the transaction data comprise one or more zero-knowledge range proofs that values of the transaction data are within respective ranges.

4. The method of claim 1,

wherein the cryptographic commitment scheme comprises a Pedersen Commitment scheme;

wherein generating one or more commitment values of a blockchain confidential transaction of the client node by applying a cryptographic commitment scheme to transaction data comprises generating the one or more commitment values of the blockchain confidential transaction of the client node based on the transaction data and random numbers corresponding to the transaction data; and

wherein generating encrypted transaction information of the blockchain confidential transaction comprises generating encrypted transaction information of the

blockchain confidential transaction by encrypting the transaction data and random numbers corresponding to the transaction data using the secret key.

5. The method of claim 1, wherein the threshold secret sharing scheme comprises a Shamir's secret sharing scheme.

6. A computer-implemented method, the method comprising:

receiving a content of a blockchain confidential transaction of a client node, by a consensus node of a blockchain network, wherein the content of the blockchain confidential transaction comprises:

one or more commitment values of the blockchain confidential transaction generated by the client node by applying a cryptographic commitment scheme to transaction data of the blockchain confidential transaction, wherein the one or more commitment values comprise:

a first commitment value generated based on a pre-transaction account balance of the client node;

a second commitment value generated based on a transaction amount of the blockchain confidential transaction; and

a third commitment value generated based on the first commitment value and the second commitment value and corresponding to a post-transaction account balance of the client node; and

encrypted transaction information generated by encrypting the transaction data using a secret key of the client node, wherein a secret key is obtained by the client node according to a threshold secret sharing scheme with a plurality of client nodes; and

one or more zero-knowledge proofs of the transaction data;

verifying, by the consensus node of the blockchain network, that the blockchain confidential transaction is valid based on the content of the blockchain confidential transaction;

storing, by the consensus node of the blockchain network, the encrypted transaction information on a blockchain of the blockchain network;

receiving, by the consensus node, a request from the client node for retrieving the encrypted transaction information stored on the blockchain;

sending, by the consensus node, the encrypted transaction information to the client node;

determining, by the client node, that the client node does not have access to the secret key in response to determining that the secret key is no longer present in a local data storage of the client node;

recovering, by the client node, the secret key according to a threshold secret sharing scheme; and

decrypting, by the client node, the encrypted transaction information using a recovered secret key.

7. The method of claim 6, wherein the transaction data of the blockchain confidential transaction comprises one or more of an account balance of the client node before the blockchain confidential transaction, or a transaction amount of the blockchain confidential transaction.

8. The method of claim 6, wherein the one or more zero-knowledge proofs of the transaction data comprise one or more zero-knowledge range proofs that values of the transaction data are within respective ranges.

9. The method of claim 6, wherein verifying that the blockchain confidential transaction is valid based on the content of the blockchain confidential transaction comprises:

determining that the one or more commitment values are correct based on the cryptographic commitment scheme; and

verifying the one or more zero-knowledge proofs of the transaction data.

10. The method of claim 9, wherein verifying the one or more zero-knowledge proofs of the transaction data comprises:

determining that an account balance of the client node before the blockchain confidential transaction is larger than zero; and

determining that a transaction amount of the blockchain confidential transaction is less than or equal to an account balance of the client node before the blockchain confidential transaction.

11. The method of claim 6, wherein the cryptographic commitment scheme is homomorphic, and the method further comprises updating an account balance of the client node after the blockchain confidential transaction based on homomorphism of the cryptographic commitment scheme.

12. The method of claim 6, wherein the threshold secret sharing scheme comprises a Shamir's secret sharing scheme.

13. The method of claim 1, wherein decrypting the encrypted transaction information using the recovered secret key comprises recovering the transaction amount of the blockchain confidential transaction using the secret key.

14. The method of claim 1, wherein decrypting the encrypted transaction information using the recovered secret key comprises recovering both the transaction amount of the blockchain confidential transaction and a random number corresponding to the transaction amount using the recovered secret key, wherein the transaction amount and the random number are used in a Pedersen Commitment scheme for concealing transaction information of the blockchain confidential transaction.

15. A non-transitory computer-readable storage medium coupled to one or more processors and having instructions stored thereon which, when executed by the one or more processors, cause the one or more processors to perform operations in accordance with the method of one or more of claims 1-14.

16. A system, comprising:

a computing device; and

a computer-readable storage device coupled to the computing device and having instructions stored thereon which, when executed by the computing device, cause the computing device to perform operations in accordance with the method of one or more of claims 1-14.