

## WHAT IS CLAIMED IS:

1. A computer-implemented method of a client node participating in a blockchain confidential transaction, the method comprising:
  - 5 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 confidential transaction of the client node by applying a cryptographic commitment scheme to transaction data;
  - generating encrypted transaction information of the confidential transaction by
  - 10 encrypting the transaction data using the secret key; and
  - transmitting, to a consensus node of a blockchain network, a content of the confidential transaction for execution, wherein the content of the confidential transaction comprises:
    - the one or more commitment values;
    - 15 the encrypted transaction information; and
    - one or more zero-knowledge proofs of the transaction data.
2. The method of claim 1, wherein the transaction data of the confidential transaction comprises one or both of an account balance of the client node before the
- 20 confidential transaction or a transaction amount of the 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.
- 25 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 confidential transaction
  - 30 of the client node by applying a cryptographic commitment scheme to transaction data comprises generating the one or more commitment values of the 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 confidential transaction comprises generating encrypted transaction information of the 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 of a consensus node of a blockchain network, the method comprising:

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

one or more commitment values of the confidential transaction generated by the client node by applying a cryptographic commitment scheme to transaction data of the confidential transaction; 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 confidential transaction is valid based on the content of the confidential transaction; and

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

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

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

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

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

10

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 confidential transaction is larger than zero; and

15 determining that a transaction amount of the confidential transaction is less than or equal to an account balance of the client node before the 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 confidential transaction based on homomorphism of the commitment scheme.

20

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

25

13. A computer-implemented method for recovering encrypted transaction information in blockchain confidential transactions, the method comprising:

receiving, by a particular client node from a consensus node of a blockchain network, encrypted transaction information of a confidential transaction of the particular client node, wherein the encrypted transaction information is stored in at least one blockchain in the blockchain network, wherein the particular client node does not have

30

access to a secret key configured to decrypt the encrypted transaction information, and where the particular client node was previously issued the secret key;

recovering, by the particular client node, the secret key from at least a threshold number of client nodes among a plurality of client nodes on the blockchain network,  
5 according to a threshold secret sharing scheme agreed to by the plurality of client nodes;  
and

decrypting, by the particular client node, transaction data of the confidential transaction of the particular client node from the encrypted transaction information using the recovered secret key.

10

14. The method of claim 13, wherein the threshold secret sharing scheme comprises a Shamir's secret sharing scheme.

15. The method of claim 13, wherein decrypting transaction data of the confidential transaction of the particular client node from the encrypted transaction information using the secret key comprises recovering a transfer amount of the confidential transaction using the secret key.

16. The method of claim 11, wherein decrypting transaction data of the confidential transaction of the particular client node from the encrypted transaction information using the secret key comprises recovering both a transfer amount of the confidential transaction and a random number corresponding to the transfer amount using the secret key, wherein the transfer amount and the random number are used in a Pedersen Commitment scheme for concealing transaction information of the confidential transaction of the particular  
25 client node.

17. 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  
30 with the method of one or more of claims 1-16.

18. 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  
5 computing device to perform operations in accordance with the method of one or more of  
claims 1-16.