

WHAT IS CLAIMED IS:

1. A computer-implemented information protection method, comprising:
obtaining a plurality of encrypted transaction amounts associated with transactions among a plurality of accounts, wherein:
each of the encrypted transaction amounts is associated with one of the accounts that sends or receives one of the transaction amounts, and
the encryption of each of the transaction amounts at least conceals whether the one account sends or receives the one of the transaction amounts;
generating a sum proof based on the obtained encrypted transaction amounts, the sum proof at least indicating that the transaction amounts are balanced; and
transmitting the encrypted transaction amounts and the sum proof to one or more nodes on a blockchain network for the nodes to verify the transactions.
2. The method of claim 1, wherein the encryption of each of the transaction amounts at least conceals whether the one account sends or receives the one of the transaction amounts by hiding whether each of the transaction amounts is inbound or outbound to the one account.
3. The method of claim 1, before generating the sum proof, further comprising:
obtaining a plurality of range proofs respectively for the accounts involved in the transactions, the range proofs at least indicating that each of the accounts that sends the transaction amounts has sufficient asset.
4. The method of claim 3, before transmitting the encrypted transaction amounts and the sum proof to the one or more nodes, further comprising: obtaining a plurality of signatures respectively from the accounts, wherein:
transmitting the encrypted transaction amounts and the sum proof to the one or more nodes on the blockchain network for the nodes to verify the transactions comprises transmitting the encrypted transaction amounts, the range proofs, the sum proof, and the signatures to the one or more nodes on the blockchain network for the nodes to verify the transactions based on the encrypted transaction amounts, the range proofs, the sum proof, and the signatures.

5. The method of claim 4, wherein transmitting the encrypted transaction amounts, the range proofs, the sum proof, and the signatures to the one or more nodes on the blockchain network for the nodes to verify the transactions based on the encrypted transaction amounts, the range proofs, the sum proof, and the signatures comprises:

transmitting the encrypted transaction amounts, the range proofs, the sum proof, and the signatures to the one or more nodes on the blockchain network; and

causing the nodes to:

validate the encrypted transaction amounts, the range proofs, the sum proof, and the signatures,

execute the transactions in response to successfully verifying the transactions, and

add the transactions into a new data block of a blockchain maintained by the blockchain network.

6. The method of claim 5, wherein causing the nodes to execute the transactions in response to successfully verifying the transactions comprises:

causing the nodes to deduct the encrypted transaction amounts correspondingly from encrypted account balances of the accounts in response to successfully verifying the transactions.

7. The method of claim 1, wherein the encryption of each of the transaction amounts comprises a homomorphic encryption.

8. The method of claim 1, wherein the encryption of each of the transaction amounts comprises a Pedersen Commitment scheme.

9. An information protection system, comprising: one or more processors and one or more non-transitory computer-readable memories coupled to the one or more processors and configured with instructions executable by the one or more processors to cause the system to perform operations comprising:

obtaining a plurality of encrypted transaction amounts associated with transactions among a plurality of accounts, wherein:

each of the encrypted transaction amounts is associated with one of the accounts that sends or receives one of the transaction amounts, and

the encryption of each of the transaction amounts at least conceals whether the one account sends or receives the one of the transaction amounts;

generating a sum proof based on the obtained encrypted transaction amounts, the sum proof at least indicating that the transaction amounts are balanced; and

transmitting the encrypted transaction amounts and the sum proof to one or more nodes on a blockchain network for the nodes to verify the transactions.

10. The system of claim 9, wherein the encryption of each of the transaction amounts at least conceals whether the one account sends or receives the one of the transaction amounts by hiding whether each of the transaction amounts is inbound or outbound to the one account.

11. The system of claim 9, wherein before generating the sum proof, the operations further comprise:

obtaining a plurality of range proofs respectively for the accounts involved in the transactions, the range proofs at least indicating that each of the accounts that sends the transaction amounts has sufficient asset.

12. The system of claim 11, wherein:

before transmitting the encrypted transaction amounts and the sum proof to the one or more nodes, the operations further comprise: obtaining a plurality of signatures respectively for the accounts; and

transmitting the encrypted transaction amounts and the sum proof to the one or more nodes on the blockchain network for the nodes to verify the transactions comprises transmitting the encrypted transaction amounts, the range proofs, the sum proof, and the signatures to the one or more nodes on the blockchain network for the nodes to verify the transactions based on the encrypted transaction amounts, the range proofs, the sum proof, and the signatures.

13. The system of claim 12, wherein transmitting the encrypted transaction amounts, the range proofs, the sum proof, and the signatures to the one or more nodes on the blockchain network for the nodes to verify the transactions based on the encrypted transaction amounts, the range proofs, the sum proof, and the signatures comprises:

transmitting the encrypted transaction amounts, the range proofs, the sum proof, and the signatures to the one or more nodes on the blockchain network; and

causing the nodes to:

validate the encrypted transaction amounts, the range proofs, the sum proof, and the signatures,

execute the transactions in response to successfully verifying the transactions, and

add the transactions into a new data block of a blockchain maintained by the blockchain network.

14. The system of claim 13, wherein causing the nodes to execute the transactions in response to successfully verifying the transactions comprises:

causing the nodes to deduct the encrypted transaction amounts correspondingly from encrypted account balances of the accounts in response to successfully verifying the transactions.

15. The system of claim 9, wherein the encryption of each of the transaction amounts comprises a homomorphic encryption.

16. The system of claim 9, wherein the encryption of each of the transaction amounts comprises a Pedersen Commitment scheme.

17. A non-transitory computer-readable storage medium configured with instructions executable by one or more processors to cause the one or more processors to perform operations comprising:

obtaining a plurality of encrypted transaction amounts associated with transactions among a plurality of accounts, wherein:

each of the encrypted transaction amounts is associated with one of the accounts that sends or receives one of the transaction amounts, and

the encryption of each of the transaction amounts at least conceals whether the one account sends or receives the one of the transaction amounts;

generating a sum proof based on the obtained encrypted transaction amounts, the sum proof at least indicating that the transaction amounts are balanced; and

transmitting the encrypted transaction amounts and the sum proof to one or more nodes on a blockchain network for the nodes to verify the transactions.

18. The storage medium of claim 17, wherein the encryption of each of the transaction amounts at least conceals whether the one account sends or receives the one of the transaction amounts by hiding whether each of the transaction amounts is inbound or outbound to the one account.

19. The storage medium of claim 17, wherein:

before generating the sum proof, the operations further comprise: obtaining a plurality of range proofs respectively for the accounts involved in the transactions, the range proofs at least indicating that each of the accounts that sends the transaction amounts has sufficient asset;

before transmitting the encrypted transaction amounts and the sum proof to the one or more nodes, the operations further comprise: obtaining a plurality of signatures respectively for the accounts; and

transmitting the encrypted transaction amounts and the sum proof to the one or more nodes on the blockchain network for the nodes to verify the transactions comprises transmitting the encrypted transaction amounts, the range proofs, the sum proof, and the signatures to the one or more nodes on the blockchain network for the nodes to verify the transactions based on the encrypted transaction amounts, the range proofs, the sum proof, and the signatures.

20. The storage medium of claim 19, wherein: transmitting the encrypted transaction amounts, the range proofs, the sum proof, and the signatures to the one or more nodes on the blockchain network for the nodes to verify the transactions based on the encrypted transaction amounts, the range proofs, the sum proof, and the signatures comprises:

transmitting the encrypted transaction amounts, the range proofs, the sum proof, and the signatures to the one or more nodes on the blockchain network; and

causing the nodes to:

validate the encrypted transaction amounts, the range proofs, the sum proof, and the signatures,

execute the transactions in response to successfully verifying the transactions, and

add the transactions into a new data block of a blockchain maintained by the blockchain network.