

What is claimed is:

1. A method for implementing blockchain-based transactions, implementable by a computing device, the method comprising:

selecting one or more blockchain assets from a remitter's blockchain account according to a transaction amount of a transaction to be remitted from the remitter's blockchain account into a receiver's blockchain account, wherein a total asset amount represented by the selected one or more blockchain assets is not less than the transaction amount, and a commitment of an individual asset amount represented by each of the selected one or more blockchain assets is recorded in a blockchain;

generating a commitment of the transaction amount; and

submitting to the blockchain the transaction comprising information of the selected one or more blockchain assets and the commitment of the transaction amount, for the selected one or more blockchain assets to be removed from the remitter's blockchain account and one or more blockchain assets corresponding to the commitment of the transaction amount to be added to the receiver's blockchain account.

2. The method of claim 1, wherein the commitment of the transaction amount is obtained by applying an encryption algorithm to the transaction amount and a transaction random number, and wherein the computing device is associated with the remitter, and the method further comprises:

before submitting the transaction to the blockchain, sending the transaction random number to another computing device associated with the receiver via an off-chain channel for the computing device associated with the receiver to determine, according to the encryption algorithm and the transaction random number, a transaction asset amount represented by the one or more blockchain assets to be added to the receiver's blockchain account.

3. The method of claim 2, wherein the encryption algorithm is Pederson Commitment.

4. The method of any of the claims 2-3, before submitting the transaction to the blockchain, further comprising:

sending the commitment of the transaction amount to the computing device associated with the receiver via an off-chain channel for the computing device associated with the receiver to verify an association among the commitment of the transaction amount, the

transaction random number, and the transaction amount.

5. The method of claim 4, before submitting the transaction to the blockchain, further comprising:

obtaining a receiver signature generated by the computing device associated with the receiver based on a receiver private key after successfully verifying the association, wherein the receiver signature represents the receiver's endorsement for the commitment of the transaction amount; and

adding the receiver signature to the transaction for blockchain nodes in the blockchain to verify the receiver signature.

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

generating a remitter signature related to the commitment of the transaction amount via a remitter private key; and

adding the remitter signature to the transaction for blockchain nodes in the blockchain to verify the remitter signature.

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

generating a range proof, wherein the range proof is related to the transaction amount; and

adding the range proof to the transaction.

8. The method of any preceding claim, before submitting the transaction to the blockchain, further comprising:

generating a commitment of a change amount in response to the total asset amount represented by the selected one or more blockchain assets being more than the transaction amount, wherein the change amount is a difference between the total asset amount of the selected one or more blockchain assets and the transaction amount; and

adding the commitment of the change amount to the transaction, for one or more blockchain assets corresponding to the commitment of the change amount to be credited back to the remitter's blockchain account.

9. The method of claim 8, wherein:

the commitment of the individual asset amount (M_i) is obtained by applying a

homomorphic encryption algorithm to the individual asset amount (p_i) and an asset random number (r_i), wherein $0 < i \leq k$ and k is the number of the selected one or more blockchain assets;

the commitment of the transaction amount (T) is obtained by applying the homomorphic encryption algorithm to the transaction amount (t) and a transaction random number (r);

the commitment of the change amount (T_0) is obtained by applying the homomorphic encryption algorithm to the change amount (t_0) and a change random number (r_0); and

before submitting the transaction to the blockchain, the method further comprises:

generating a verification random number (r'), wherein $r' = r_1 + \dots + r_k - r_0$; and

adding the verification random number (r') to the transaction for blockchain nodes in the blockchain to verify whether an input of the transaction is equal to an output of the transaction.

10. The method of claim 9, wherein the input of the transaction is verified to be equal to the output of the transaction in response to a verification commitment (R') corresponding to the verification random number r' is equal to $M_1 + \dots + M_k - T - T_0$.

11. The method of claim 8, wherein the commitment of the change amount is obtained by applying the homomorphic encryption algorithm to the change amount and a change random number.

12. The method of claim 11, before submitting the transaction to the blockchain, further comprising:

generating a range proof, wherein the range proof is related to the change amount; and

adding the range proof to the transaction.

13. A system for implementing blockchain-based 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 the claims 1 to 12.

14. An apparatus for implementing blockchain-based transactions, comprising a plurality of modules for performing the method of any of the claims 1 to 12.

15. 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 the method of any of the claims 1 to 12.