## Claims

1. A computer-implemented method for implementing blockchain-based transactions, comprising:

determining a transaction amount to be remitted from a remitter's blockchain account into a receiver's blockchain account, wherein a balance of the remitter's blockchain account comprises a plurality of reserve balances, and a commitment of each of the plurality of reserve balances is recorded in a blockchain;

selecting one or more of the plurality of reserve balances from the remitter's blockchain account, wherein the sum of the selected one or more of the plurality of reserve balances is not smaller than the transaction amount; and

submitting to the blockchain a transaction comprising an identification of each of the selected one or more of the plurality of reserve balances and a commitment of the transaction amount, for the selected one or more of the plurality of reserve balances to be removed from the remitter's blockchain account and the transaction amount to be added to the receiver's blockchain account after the transaction is implemented.

2. The computer-implemented method of claim 1, wherein the balance of the remitter's blockchain account further comprises a first inward remittance balance; the method further comprises:

in response to that the balance of the remitter's blockchain account increases, adding a corresponding amount to the first inward remittance balance.

3. The computer-implemented method of claim 2, wherein, in response to that the sum of the selected one or more of the plurality of reserve balances is greater than the transaction amount, a change amount is added to the first inward remittance balance after the transaction is implemented, and wherein the change amount is the difference between the sum of the selected one or more of the plurality of reserve balances and the transaction amount.

4. The computer-implemented method of any of the claims 2-3, wherein the balance of the remitter's blockchain account further comprises an outward remittance balance, and the outward remittance balance comprises the plurality of the reserve balances.

5. The computer-implemented method of claim 4, further comprising:

converting at least one part of the first inward remittance balance to the outward remittance balance.

6. The computer-implemented method of any preceding claim, wherein a balance of the

receiver's blockchain account comprises a second inward remittance balance, and a commitment of the second inward remittance balance is recorded in the blockchain; and wherein the commitment of the transaction amount is added to the commitment of the second inward remittance balance after the transaction is implemented.

7. The computer-implemented method of claim 6, wherein the commitment of the transaction amount is an encryption of the transaction amount based on a transaction random number, and the commitment of the second inward remittance balance is an encryption of the second inward remittance balance based on an inward remittance balance random number.

8. The computer-implemented method of any of the claims 6-7, wherein the method is implementable by a first computing device associated with the remitter, and the method further comprises:

sending the transaction random number to a second computing device associated with the receiver via an off-chain channel for the second computing device associated with the receiver to determine an updated second inward remittance balance according to an updated commitment of the second inward remittance balance and an updated inward remittance balance random number;

wherein the updated commitment of the second inward remittance balance is obtained by adding the commitment of the transaction amount to the commitment of the second inward remittance balance, the updated inward remittance balance random number is obtained by adding the transaction random number to the inward remittance balance random number, and the updated second inward remittance balance is the sum of the second inward remittance balance and the transaction amount.

9. The computer-implemented method of claim 8, before submitting to the blockchain the transaction, the method further comprises:

sending the commitment of the transaction amount to the second computing device associated with the receiver via an off-chain channel for the second 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.

10. The computer-implemented method of any of the claims 8-9, further comprising:

obtaining a receiver signature endorsing the commitment of the transaction amount, wherein the receiver signature is generated by the second computing device associated with the receiver based on a receiver private key, in response to successful verification of the association; and

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

11. The computer-implemented method of any preceding claim, further comprising:

generating a remitter signature endorsing the commitment of the transaction amount based on a remitter private key; and

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

12. The computer-implemented method of any preceding claim, further comprising:

generating a range proof; and

adding the range proof to the transaction for a plurality of blockchain nodes in the blockchain to verify that the sum of the selected one or more of the plurality of reserve balances is not smaller than the transaction amount.

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 claims 1 to 12.

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