

What is claimed is:

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

determining a transaction amount to be remitted from a blockchain account of a remitter into a blockchain account of a receiver, wherein the blockchain account of the remitter records a homomorphic encryption ciphertext of the remitter's balance in a blockchain, and the blockchain account of the receiver records a homomorphic encryption ciphertext of the receiver's balance in the blockchain;

generating a homomorphic encryption ciphertext of the transaction amount with respect to the remitter and a homomorphic encryption ciphertext of the transaction amount with respect to the receiver; and

submitting to the blockchain a transaction comprising information of the blockchain account of the remitter, information of the blockchain account of the receiver, the homomorphic encryption ciphertext of the transaction amount with respect to the remitter and the homomorphic encryption ciphertext of the transaction amount with respect to the receiver, for the homomorphic encryption ciphertext of the transaction amount with respect to the remitter to be subtracted from the homomorphic encryption ciphertext of the remitter's balance and for the homomorphic encryption ciphertext of the transaction amount with respect to the receiver to be added to the homomorphic encryption ciphertext of the receiver's balance.

2. The computer-implemented method of claim 1, wherein the homomorphic encryption ciphertext of the remitter's balance is a commitment of the remitter's balance, and the homomorphic encryption ciphertext of the receiver's balance is a commitment of the receiver's balance.

3. The computer-implemented method of any of the claims 1-2, wherein the homomorphic encryption ciphertext of the remitter's balance is a Pedersen Commitment of the remitter's balance, and the homomorphic encryption ciphertext of the receiver's balance is a Pedersen Commitment of the receiver's balance.

4. The computer-implemented method of any preceding claim, wherein the homomorphic encryption ciphertext of the remitter's balance is obtained by applying a homomorphic encryption algorithm to the remitter's balance based on a public key of the remitter and a remitter random number, and the homomorphic encryption ciphertext of the

receiver's balance is obtained by applying a homomorphic encryption algorithm to the receiver's balance based on a public key of the receiver and a receiver random number.

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

generating a range proof related to the remitter's balance and the transaction amount with respect to the remitter; and

adding the range proof to the transaction for the one or more blockchain nodes in the blockchain to verify whether the transaction amount is no greater than the remitter's balance.

6. The computer-implemented method of any preceding claim, wherein the homomorphic encryption ciphertext of the transaction amount with respect to the remitter is a commitment of the transaction amount with respect to the remitter based on the public key of the remitter, and the homomorphic encryption ciphertext of the transaction amount with respect to the receiver is a commitment of the transaction amount with respect to the receiver based on the public key of the receiver.

7. The computer-implemented method of claim 6, further comprising:

applying a homomorphic encryption algorithm to generate the commitment of the transaction amount with respect to the remitter based on a transaction amount random number with respect to the remitter, the transaction amount, and the public key of the remitter; and

applying the homomorphic encryption algorithm to generate the commitment of the transaction amount with respect to the receiver based on a transaction amount random number with respect to the receiver, the transaction amount, and the public key of the receiver.

8. The computer-implemented method of claim 7, further comprising:

determining a difference between the transaction amount random number with respect to the remitter and the transaction amount random number with respect to the receiver; and

adding the difference between the transaction amount random number with respect to the remitter and the transaction amount random number with respect to the receiver in the transaction, for one or more blockchain nodes in the blockchain to verify that the commitment of the transaction amount with respect to the remitter is equal to the commitment of the transaction amount with respect to the receiver.

9. The computer-implemented method of any of the claim 7-8, wherein the method is

implementable by a first computing device associated with the remitter, and the method further comprises:

sending the transaction amount random number with respect to the receiver to a second computing device associated with the receiver via an off-chain channel.

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

generating a public key proof associated with the receiver according to a homomorphic encryption algorithm and the homomorphic encryption ciphertext of the transaction amount with respect to the receiver; and

adding the public key proof associated with the receiver in the transaction, for one or more blockchain nodes in the blockchain to verify that the homomorphic encryption ciphertext of the transaction amount with respect to the receiver and the homomorphic encryption ciphertext of the receiver's balance are both encrypted based on the public key of the receiver.

11. The computer-implemented method of claim 10, wherein generating a public key proof associated with the receiver according to a homomorphic encryption algorithm and the homomorphic encryption ciphertext of the transaction amount with respect to the receiver comprises:

generating a first verification random number and a second verification random number;

applying the homomorphic encryption algorithm to generate a random-number homomorphic encryption ciphertext based on the first verification random number, the second verification random number, and the public key of the receiver;

obtaining a hash digest by conducting a hash operation on the homomorphic encryption ciphertext of the transaction amount with respect to the receiver and the random-number homomorphic encryption ciphertext; and

generating a first verification element associated with the first verification random number and a second verification element associated with the second verification random number according to the hash digest.

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

generating a digital signature of the remitter endorsing the homomorphic encryption ciphertext of the transaction amount with respect to the remitter and the homomorphic encryption ciphertext of the transaction amount with respect to the receiver based on a private

key of the remitter; and

adding the digital signature of the remitter to the transaction for one or more blockchain nodes in the blockchain to verify the digital signature of the remitter.

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 computer-implemented method of any of claims 1 to 12.

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