What is claimed is:

1. A blockchain-based transaction method, applicable at a remitter's equipment, the method comprising:

determining a transaction amount to be remitted from a blockchain account of the remitter into a blockchain account of a receiver, wherein the blockchain account of the remitter records a commitment ciphertext of the remitter's balance in a blockchain, and the blockchain account of the receiver records a commitment ciphertext of the receiver's balance in the blockchain, wherein the commitment ciphertext of the remitter's balance is obtained by applying a homomorphic encryption algorithm based on the remitter's balance and a public key of the remitter, and the commitment ciphertext of the receiver's balance is obtained by applying the homomorphic encryption algorithm based on the receiver's balance and a public key of the receiver;

generating a commitment ciphertext of the transaction amount with respect to the remitter and a commitment ciphertext of the transaction amount with respect to the receiver, wherein the commitment ciphertext of the transaction amount with respect to the remitter is generated by applying the homomorphic encryption algorithm based on the transaction amount and the public key of the remitter, and the commitment ciphertext of the transaction amount with respect to the receiver is generated by applying the homomorphic encryption algorithm based on the transaction amount and the public key of 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 commitment ciphertext of the transaction amount with respect to the remitter, and the commitment ciphertext of the transaction amount with respect to the receiver, for the commitment ciphertext of the transaction amount with respect to the remitter to be subtracted from the commitment ciphertext of the remitter's balance and for the commitment ciphertext of the transaction amount with respect to the receiver to be added to the commitment ciphertext of the receiver's balance;

the method further comprising:

generating a public key proof associated with the receiver, wherein the public key proof associated with the receiver is generated by applying the homomorphic encryption algorithm

based on the commitment 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 commitment ciphertext of the transaction amount with respect to the receiver and the commitment ciphertext of the receiver's balance are both obtained by applying the homomorphic encryption algorithm based on the public key of the receiver.

2. The method of claim 1, wherein:

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

the commitment ciphertext of the transaction amount with respect to the receiver is generated by applying the homomorphic encryption algorithm based on a transaction amount random number with respect to the receiver, the transaction amount, and the public key of the receiver,

the method further comprising:

generating 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 transaction amount encrypted in the commitment ciphertext of the transaction amount with respect to the remitter is equal to the transaction amount encrypted in the commitment ciphertext of the transaction amount with respect to the receiver.

3. The method of claim 1, wherein generating the public key proof associated with 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 commitment 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 commitment ciphertext of the transaction amount with respect to the receiver and the random-number commitment 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,

wherein the public key proof associated with the receiver comprises the random-number commitment ciphertext, the first verification element, and the second verification element.

4. The method of claim 3, wherein the commitment ciphertext of the remitter's balance is obtained by applying the homomorphic encryption algorithm based on the remitter's balance, a public key of the remitter, and a remitter random number;

the method further comprising:

generating a range proof based on the remitter random number, the transaction amount random number with respect to the remitter, the remitter's balance, the commitment ciphertext of the remitter's balance, the transaction amount, and the commitment ciphertext of 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 satisfies: the transaction amount being no less than 0 and no greater than the remitter's balance.

5. The method of any one of claims 1-4, further comprising:

generating, based on a private key of the remitter, a digital signature of the remitter related to the commitment ciphertext of the transaction amount with respect to the remitter and

the commitment ciphertext of the transaction amount with respect to the receiver; and

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

6. The method of claim 2, further comprising:

sending the transaction amount random number with respect to the receiver to the receiver via an off-chain channel.

7. A blockchain-based transaction device, applicable at a remitter's equipment, the device comprising:

a determining unit determining a transaction amount to be remitted from a blockchain account of the remitter into a blockchain account of a receiver, wherein the blockchain account of the remitter records a commitment ciphertext of the remitter's balance in a blockchain, and the blockchain account of the receiver records a commitment ciphertext of the receiver's balance in the blockchain, wherein the commitment ciphertext of the remitter's balance is obtained by applying a homomorphic encryption algorithm based on the remitter's balance and a public key of the remitter, and the commitment ciphertext of the receiver's balance is obtained by applying the homomorphic encryption algorithm based on the receiver's balance and a public key of the receiver;

a generating unit generating a commitment ciphertext of the transaction amount with respect to the remitter and a commitment ciphertext of the transaction amount with respect to the receiver, wherein the commitment ciphertext of the transaction amount with respect to the remitter is generated by applying the homomorphic encryption algorithm based on the transaction amount and the public key of the remitter, and the commitment ciphertext of the transaction amount with respect to the receiver is generated by applying the homomorphic encryption algorithm based on the transaction amount and the public key of the receiver; and

a submitting unit submitting to the blockchain a transaction comprising information of the blockchain account of the remitter, information of the blockchain account of the receiver, the commitment ciphertext of the transaction amount with respect to the remitter, and the

commitment ciphertext of the transaction amount with respect to the receiver, for the commitment ciphertext of the transaction amount with respect to the remitter to be subtracted from the commitment ciphertext of the remitter's balance and for the commitment ciphertext of the transaction amount with respect to the receiver to be added to the commitment ciphertext of the receiver's balance;

wherein the generating unit:

generating a public key proof associated with the receiver, wherein the public key proof associated with the receiver is generated by applying the homomorphic encryption algorithm based on the commitment 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 commitment ciphertext of the transaction amount with respect to the receiver and the commitment ciphertext of the receiver's balance are both obtained by applying the homomorphic encryption algorithm based on the public key of the receiver.

8. The device of claim 7, wherein:

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

the commitment ciphertext of the transaction amount with respect to the receiver is generated by applying the homomorphic encryption algorithm based on a transaction amount random number with respect to the receiver, the transaction amount, and the public key of the receiver,

the generating unit:

generating 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 transaction amount encrypted in the commitment ciphertext of the transaction amount with respect to the remitter is equal to the transaction amount encrypted in the commitment ciphertext of the transaction amount with respect to the receiver.

9. The device of claim 7, wherein the generating unit:

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

applying the homomorphic encryption algorithm to generate a random-number commitment 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 commitment ciphertext of the transaction amount with respect to the receiver and the random-number commitment 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,

wherein the public key proof associated with the receiver comprises the random-number commitment ciphertext, the first verification element, and the second verification element.

10. The device of claim 9, wherein the commitment ciphertext of the remitter's balance is obtained by applying the homomorphic encryption algorithm based on the remitter's balance, a public key of the remitter, and a remitter random number;

the generating unit:

generating a range proof based on the remitter random number, the transaction amount random number with respect to the remitter, the remitter's balance, the commitment ciphertext of the remitter's balance, the transaction amount, and the commitment ciphertext of 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 satisfies: the transaction amount being no less than 0 and no greater than the remitter's balance.

11. The device of any one of claims 7-10, wherein the generating unit:

generating, based on a private key of the remitter, a digital signature of the remitter related to the commitment ciphertext of the transaction amount with respect to the remitter and the commitment ciphertext of the transaction amount with respect to the receiver; and

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

12. The device of claim 8, further comprising:

an off-chain sending unit sending the transaction amount random number with respect to the receiver to the receiver via an off-chain channel.

13. A computer device, comprising: a storage device and a processor, the storage device storing computer programs executable by the processor which, when executing the computer programs, performs the method of any of claims 1 to 6.