CLAIMS

What is claimed is:

1. A method for transferring an asset, applied to, the method comprising:

receiving, by a node device of a blockchain, an asset transfer transaction sent by an asset transferor, wherein the asset transfer transaction comprises a commitment value that is generated through calculation by inputting at least an asset type of an output asset object in the asset transfer transaction as input data to a commitment function, and a proof used to perform a zero-knowledge proof on the commitment value;

performing the zero-knowledge proof on the commitment value based on the proof;

verifying whether an asset type of an input asset object matches the asset type of the output asset object in the asset transfer transaction; and

in response to verifying that the asset type of the input asset object matches the asset type of the output asset object in the asset transfer transaction, publishing the commitment value corresponding to the output asset object on the blockchain for deposit.

2. The method according to claim 1, further comprising:

in response to verifying that the asset type of the input asset object matches the asset type of the output asset object in the asset transfer transaction, publishing identifier information corresponding to the commitment value of the input asset object on the blockchain for deposit.

3. The method according to claim 1, wherein the proof is generated through calculation by the asset transferor by inputting at least the commitment value, the asset type of the input asset object, and the asset type of the output asset object as input data to a proof generation algorithm comprised in the blockchain.

4. The method according to claim 3, wherein the blockchain supports hiding related information of the input asset object.

5. The method according to claim 4, wherein the input data of the proof generation algorithm comprises the commitment value, the asset type of the input asset object, the asset type of the output asset object, and identifier information corresponding to the commitment value of the input asset object.

6. The method according to claim 5, wherein performing the zero-knowledge proof on the commitment value based on the proof, to verify whether the asset type of the input asset object matches the asset type of the output asset object in the asset transfer transaction comprises:

performing the zero-knowledge proof on the commitment value based on the proof, to verify whether the identifier information corresponds to the commitment value of an asset object deposited in the blockchain, and to verify whether the asset type of the input asset object matches the asset type of the output asset object in the asset transfer transaction.

7. The method according to claim 6, wherein performing the zero-knowledge proof on the commitment value based on the proof, to verify whether the asset type of the input asset object matches the asset type of the output asset object in the asset transfer transaction comprises:

inputting at least the proof and the commitment value as input data of a proof verification algorithm to the proof verification algorithm for calculation; and

verifying whether the identifier information corresponds to the commitment value of the asset object deposited in the blockchain, and verifying whether the asset type of the input asset object matches the asset type of the output asset object in the asset transfer transaction, based on an output result of the proof verification algorithm.

8. The method according to claim 1, wherein the commitment function is a hash function.

9. The method according to claim 1, wherein the zero-knowledge proof is based on an algorithm comprising a zksnark algorithm or a zkstark algorithm.

10. The method according to claim 1, wherein the blockchain comprises a consortium blockchain, a private chain or a public chain.

11. The method according to claim 1, wherein the blockchain comprises a key generation algorithm.

12. The method according to claim 1, further comprising:
receiving a public key of an asset receiver.

13. An apparatus for transferring an asset, the apparatus comprising a plurality of modules configured to perform the method of any one of claims 1 to 12.