

CLAIMS

What is claimed is:

1. A method for blockchain-based asset issuance, the method comprising:
 - receiving, by a node device in a blockchain, an asset issuance transaction sent by an asset issuer, wherein the asset issuance transaction comprises a commitment value and a proof for performing a zero-knowledge proof with respect to the commitment value, and wherein the commitment value is calculated by inputting at least an asset type of a target asset object issued by the asset issuer as input data to a commitment function;
 - initiating the zero-knowledge proof with respect to the commitment value based on the proof;
 - verifying that the asset type of the target asset object is a legal asset type allowed to be issued by the asset issuer; and
 - if the verification result is YES, issuing the commitment value to the blockchain for storage.
2. The method of claim 1, wherein the proof is generated by calculating via a proof generation algorithm implemented in the blockchain with inputting, by the asset issuer, at least the commitment value and the legal asset type allowed to be issued by the asset issuer as input data.
3. The method of claim 1, wherein
 - the node device maintains a verification rule for verifying whether the asset type of the target asset object is the legal asset type allowed to be issued by the asset issuer; and
 - wherein the proof is generated by calculating via a proof generation algorithm implemented in the blockchain with inputting, by the asset issuer, at least verification data related to the verification rule as input data.
4. The method of claim 1, further comprising:
 - determining whether the blockchain supports hiding identity information of the asset issuer, and
 - in response to determining that the blockchain supports hiding identity information of the asset issuer, the input data to the proof generation algorithm further includes a private key of the asset issuer.

5. The method of claim 4, wherein initiating the zero-knowledge proof with respect to the commitment value based on the proof, comprises:

in response to determining that the blockchain does not support hiding identity information of the asset issuer, initiating the zero-knowledge proof with respect to the commitment value based on the proof, so to verify whether the asset type of the target asset object is the legal asset type allowed to be issued by the asset issuer.

6. The method of claim 5, further comprising:

in response to determining that the blockchain supports hiding the identity information of the asset issuer, initiating the zero-knowledge proof with respect to the commitment value based on the proof, to verify

whether the asset issuer holds a private key corresponding to a public key of a legal asset issuer, and

whether the asset type of the target asset object is the legal asset type allowed to be issued by the legal asset issuer.

7. The method of claim 1, wherein initiating the zero-knowledge proof with respect to the commitment value based on the proof, comprises:

calculating with a proof verification algorithm by inputting at least the proof and the commitment value as input data to the proof verification algorithm; and

determining whether the asset type of the target asset object is the legal asset type allowed to be issued by the asset issuer, based on an output result from the proof verification algorithm.

8. The method of claim 1, wherein

the node device is configured with a verification rule for verifying whether the asset type of the target asset object is the legal asset type allowed to be issued by the asset issuer; and

wherein the input data further comprises verification data related to the verification rule.

9. The method of claim 8, wherein

the node device maintains an asset type list comprising legal asset types allowed to be issued by the asset issuer;

wherein the verification rule comprises:

verifying whether the asset type of the target asset object is included in the asset type list;

if the verification result is YES, determining that the asset type of the target asset object is the legal asset type allowed to be issued by the asset issuer; and

wherein the verification data comprises the asset type list.

10. The method of claim 9, wherein

the node device maintains a hash tree comprising hash values of legal asset types allowed to be issued by the asset issuer;

wherein the verification rule comprises:

verifying whether a hash value of the asset type of the target asset object is included in the hash tree;

if the verification result is YES, determining that the asset type of the target asset object is the legal asset type allowed to be issued by the asset issuer; and

wherein the verification data comprises the hash tree.

11. The method of claim 1, wherein

the node device maintains a public key list comprising public keys of all of legal asset issuers and a hash tree comprising hash values of the public keys of all of legal asset issuers;

wherein the verification rule comprises:

verifying whether a prefix or suffix of the asset type of the target asset object matches any one of follows: a public key of legal asset issuer, a prefix or suffix of the public key of legal asset issuer, a hash value of the public key of legal asset issuer, and wherein a prefix or suffix of the hash value of the public key of legal asset issuer;

if the verification result is YES, determining that the asset type of the target asset object is the legal asset type allowed to be issued by the asset issuer; and

wherein the verification data comprises the public key list or the hash tree.

12. The method of claim 1, wherein

the commitment function is a hash function, and

wherein the zero-knowledge proof is implemented in the blockchain and is a zksnark algorithm or a zkstark algorithm.

13. The method according to claim 1, wherein the commitment function is configured to prevent restoring original data from the commitment value by a reverse calculation.

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

15. An apparatus for blockchain-based asset issuance, the apparatus comprising a plurality of modules configured to perform the method of any one of claims 1 to 14.