

CLAIMS

~~What is claimed is:~~

1. A computer-implemented method for blockchain-based asset issuance, the computer-implemented method comprising:

~~receiving~~maintaining, by a node device in a blockchain, verification data corresponding to a set of legal asset types allowed to be issued by an asset issuer, wherein the node device is configured with a verification rule for determining whether an asset type of a target asset object issued by the asset issuer is in the set of legal asset types allowed to be issued by the asset issuer, and wherein the verification data is related to the verification rule;

receiving, by the node device in the blockchain and from the asset issuer, a request to generate an output of a proof generation algorithm, wherein the proof generation algorithm is implemented in the blockchain;

generating, by the node device, the output of the proof generation algorithm by supplying the proof generation algorithm with input data provided by the asset issuer, wherein the input data comprises the verification data, a commitment value and the set of legal asset types allowed to be issued by the asset issuer, and wherein the commitment value is calculated, by the asset issuer, by supplying at least the asset type of the target asset object issued by the asset issuer to a commitment function;

transmitting, by the node device, the output of the proof generation algorithm to the asset issuer for calculation of a proof of the commitment value by the asset issuer;

receiving, by the node device, an asset issuance transaction~~sent by an asset issuer,~~ wherein the asset issuance transaction comprises ~~at the~~ commitment value and ~~at the~~ 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, by the node device, a process of verifying the proof based on the verification rule, wherein the process of verifying the proof is used for the zero-knowledge proof with respect to the commitment value~~based on the proof;~~

verifying, by the node device, the proof based on the verification rule, by determining that the asset type of the target asset object is ain the set of legal asset ~~typetypes~~ allowed to be issued by the asset issuer, comprising:

determining that asset type related data of the target asset object is included in the verification data; and

~~if the verification result is YES~~in response to determining that the asset type related data of the target asset object is included in the verification data, determining that the asset type of the target asset object is in the set of legal asset types allowed to be issued by the asset issuer; and

in response to determining that the asset type of the target asset object is in the set of legal asset types allowed to be issued by the asset issuer, issuing, by the node device, the commitment value to the blockchain for storage, wherein the asset type of the target asset object issued by the asset issuer is hidden in the blockchain.

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~~computer-implemented.

4. ~~The method of claim 1, further comprising:~~

determining ~~whether~~that the blockchain supports hiding identity information of the asset issuer; and

in response to determining that the blockchain supports hiding the identity information of the asset issuer, the input data to the proof generation algorithm further ~~includes~~comprises a private key of the asset issuer.

~~5.~~

3. The computer-implemented method of claim 42, wherein ~~initiating~~determining that the asset type of the target asset object is a legal asset type allowed to be issued by the asset issuer further comprises:

determining that the private key of the asset issuer corresponds to a public key of a legal asset issuer.

4. The computer-implemented method of claim 1, wherein:
the asset type related data of the target asset object comprises the asset type of the target asset object; and
the verification data comprises an asset type list comprising the set of legal asset types allowed to be issued by the asset issuer.
5. The computer-implemented method of claim 1, wherein:
the asset type related data of the target asset object comprises a hash value of the asset type of the target asset object; and
the verification data comprises a hash tree comprising hash values of the set of legal asset types allowed to be issued by the asset issuer.
6. The computer-implemented method of claim 1, wherein:
the asset type related data of the target asset object comprises a prefix or a suffix of the asset type of the target asset object; and
the verification data comprises a public key list comprising public keys of all of legal asset issuers or a hash tree comprising hash values of the public keys of all of legal asset issuers.
7. The computer-implemented method of claim 1, further comprising:
determining, by the node device, that the asset type of the target asset object is not in the set of legal asset types allowed to be issued by the asset issuer; and
discarding, by the node device, the asset issuance transaction.
8. A non-transitory, computer-readable medium storing one or more instructions executable by a computer system to perform operations comprising:
maintaining, by a node device in a blockchain, verification data corresponding to a set of legal asset types allowed to be issued by an asset issuer, wherein the node device is configured with a verification rule for determining whether an asset type of a target asset object issued by the asset issuer is in the set of legal asset types allowed to be issued by the asset issuer, and wherein the verification data is related to the verification rule;
receiving, by the node device in the blockchain and from the asset issuer, a request to generate an output of a proof generation algorithm, wherein the proof generation algorithm is implemented in the blockchain;

generating, by the node device, the output of the proof generation algorithm by supplying the proof generation algorithm with input data provided by the asset issuer, wherein the input data comprises the verification data, a commitment value and the set of legal asset types allowed to be issued by the asset issuer, and wherein the commitment value is calculated, by the asset issuer, by supplying at least the asset type of the target asset object issued by the asset issuer to a commitment function;

transmitting, by the node device, the output of the proof generation algorithm to the asset issuer for calculation of a proof of the commitment value by the asset issuer;

receiving, by the node device, an asset issuance transaction, wherein the asset issuance transaction comprises the commitment value and the proof for performing a 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~~initiating, by the node device, a process of verifying the proof based on the verification rule, wherein the process of verifying the proof is used for 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-~~verifying, by the node device, the proof based on the verification rule, by determining that the asset type of the target asset object is in the set of legal asset types allowed to be issued by the asset issuer, comprising:

determining that asset type related data of the target asset object is included in the verification data; and

in response to determining that the asset type related data of the target asset object is included in the verification data, determining that the asset type of the target asset object is in the set of legal asset types allowed to be issued by the asset issuer; and in response to determining that the asset type of the target asset object is in the set of legal asset types allowed to be issued by the asset issuer, issuing, by the node device, the commitment value to the blockchain for storage, wherein the asset type of the target asset object issued by the asset issuer is hidden in the blockchain.

9. The ~~method~~non-transitory, computer-readable medium of claim 58, further comprising: determining that the blockchain supports hiding identity information of the asset issuer; and

in response to determining that the blockchain supports hiding the identity information of the asset issuer, ~~initiating the zero knowledge proof with respect to~~ input data to the commitment value based on proof generation algorithm further comprises a private key of the proof, to verify asset issuer.

~~whether the~~

10. The non-transitory, computer-readable medium of claim 9, wherein determining that the asset type of the target asset object is a legal asset type allowed to be issued by the asset issuer ~~holds a further comprises:~~

determining that the private key corresponding of the asset issuer corresponds to a public key of a legal asset issuer, ~~and.~~

11. ~~whether the~~ The non-transitory, computer-readable medium of claim 8, wherein:

the asset type related data of the target asset object ~~is comprises~~ the asset type of the target asset object; and

the verification data comprises an asset type list comprising the set of legal asset ~~types~~ types allowed to be issued by the asset issuer.

12. The non-transitory, computer-readable medium of claim 8, wherein:

the asset type related data of the target asset object comprises a hash value of the asset type of the target asset object; and

the verification data comprises a hash tree comprising hash values of the set of legal asset ~~types~~ types allowed to be issued by the asset issuer.

13. The ~~method~~ non-transitory, computer-readable medium of claim 8, wherein ~~initiating:~~

the asset type related data of the target asset object comprises a prefix or a suffix of the asset type of the target asset object; and

the verification data comprises a public key list comprising public keys of all of legal asset issuers or a hash tree comprising hash values of the public keys of all of legal asset issuers.

14. A computer-implemented system, comprising:

one or more computers; and

one or more computer memory devices interoperably coupled with the one or more computers and having tangible, non-transitory, machine-readable media storing one or more

instructions that, when executed by the one or more computers, perform one or more operations comprising:

maintaining, by a node device in a blockchain, verification data corresponding to a set of legal asset types allowed to be issued by an asset issuer, wherein the node device is configured with a verification rule for determining whether an asset type of a target asset object issued by the asset issuer is in the set of legal asset types allowed to be issued by the asset issuer, and wherein the verification data is related to the verification rule;

receiving, by the node device in the blockchain and from the asset issuer, a request to generate an output of a proof generation algorithm, wherein the proof generation algorithm is implemented in the blockchain;

generating, by the node device, the output of the proof generation algorithm by supplying the proof generation algorithm with input data provided by the asset issuer, wherein the input data comprises the verification data, a commitment value and the set of legal asset types allowed to be issued by the asset issuer, and wherein the commitment value is calculated, by the asset issuer, by supplying at least the asset type of the target asset object issued by the asset issuer to a commitment function;

transmitting, by the node device, the output of the proof generation algorithm to the asset issuer for calculation of a proof of the commitment value by the asset issuer;

receiving, by the node device, an asset issuance transaction, wherein the asset issuance transaction comprises the commitment value and the proof for performing a zero-knowledge proof with respect to the commitment value;

initiating, by the node device, a process of verifying the proof based on the proof, comprises: verification rule, wherein the process of verifying the proof is used for the zero-knowledge proof with respect to the commitment value;

calculating with a verifying, by the node device, the proof verification algorithm by inputting at least the proof and the commitment value as input data to based on the proof verification algorithm; and

rule, by determining whether that the asset type of the target asset object is in 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~~set of legal asset types allowed to be issued by the asset issuer;, comprising:

~~wherein the verification rule comprises:~~

~~verifying whether the~~determining that asset type related data of the target asset object is included in the asset type list;verification data; and

~~if the verification result is YES, in response to~~ 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~~related 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.~~

~~, determining that the asset type of the target asset object is in the set of~~
~~legal asset types allowed to be issued by the asset issuer; and~~

~~in response to determining that the asset type of the target asset object is in the set of legal asset types allowed to be issued by the asset issuer, issuing, by the node device, the commitment value to the blockchain for storage, wherein the asset type of the target asset object issued by the asset issuer is hidden in the blockchain.~~

15. The computer-implemented system of claim 14, further comprising:

determining that the blockchain supports hiding identity information of the asset issuer;
and

in response to determining that the blockchain supports hiding the identity information of the asset issuer, the input data to the proof generation algorithm further comprises a private key of the asset issuer.

16. The computer-implemented system of claim 15, wherein determining that the asset type of the target asset object is a legal asset type allowed to be issued by the asset issuer further comprises:

determining that the private key of the asset issuer corresponds to a public key of a legal asset issuer.

17. The computer-implemented system of claim 14, wherein:

the asset type related data of the target asset object comprises the asset type of the target asset object; and

the verification data comprises an asset type list comprising the set of legal asset types allowed to be issued by the asset issuer.

18. The computer-implemented system of claim 14, wherein:

the asset type related data of the target asset object comprises a hash value of the asset type of the target asset object; and

the verification data comprises a hash tree comprising hash values of the set of legal asset types allowed to be issued by the asset issuer.

19. The computer-implemented system of claim 14, wherein:

the asset type related data of the target asset object comprises a prefix or a suffix of the asset type of the target asset object; and

the verification data comprises

~~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/or~~ 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.~~