

CLAIMS

What is claimed is:

1. ~~An identity information authentication method, comprising:
obtaining a plurality of pieces of identity information of a user;
5 constructing, using a non-hash algorithm, a Merkle tree based on the plurality of
pieces of identity information of the user, wherein leaf nodes of the Merkle tree are
generated by encoding, using the non-hash algorithm, identity information of the user
and other data information, wherein the other data information is a random number;
and
10 transmitting, to a storage terminal, mapping relationships between the plurality
of pieces of identity information of the user and the leaf nodes, Merkle proofs of the
leaf nodes corresponding to the plurality of pieces of identity information of the user
on the Merkle tree constructed based on the plurality of pieces of identity information
of the user, a root value of the Merkle tree constructed based on the plurality of pieces
15 of identity information of the user and mapping relationships between the other data
information and the leaf nodes.~~
2. ~~The method according to claim 1, wherein the non-hash algorithm is base 64.~~
- 20 3. ~~The method according to claim 1 or 2, wherein the storage terminal comprises
one or more of a client device of the user, a server of a certification authority, or a
blockchain-based distributed database.~~
- 25 4. ~~The method according to claim 3, wherein the storage terminal comprises the
server of the certification authority; and
the root value of the Merkle tree constructed based on the plurality of pieces of
identity information of the user is stored in a digital certificate of the user by the
certification authority;
wherein the digital certificate comprises a content portion and a signature portion;
30 the content portion comprises the root value of the Merkle tree constructed based on
the plurality of pieces of identity information of the user, and the signature portion is
an electronic signature of the content portion.~~

5. ~~The method according to claim 4, wherein the content portion of the digital certificate further comprises the mapping relationships between the plurality of pieces of identity information of the user and the leaf nodes, and Merkle proofs of the leaf nodes corresponding to the plurality of pieces of identity information of the user on the Merkle tree constructed based on the plurality of pieces of identity information of the user.~~

6. ~~The method according to claim 5, wherein the storage terminal further comprises the client device of the user or a blockchain-based distributed database, and the mapping relationships between the plurality of pieces of identity information of the user and the Merkle proofs of the leaf nodes corresponding to the plurality of pieces of identity information of the user on the Merkle tree constructed based on the plurality of pieces of identity information of the user are stored in the client device of the user or the blockchain-based distributed database.~~

7. ~~The method according to claim 5, wherein the content portion of the digital certificate of the user further comprises a public key of the user.~~

8. ~~The method according to claim 1, wherein the identity information of the user comprises one or more of a public key of the user, a name of the user, an address of the user, or an identification number of the user.~~

9.1. An identity information verification method performed by an authority that needs to verify an identity information to be verified, the method comprising:

in response to the identity information to be verified, obtaining, from a storage terminal,

1) a Merkle proof of a leaf node corresponding to the identity information to be verified ~~based on mapping relationships between~~, comprising obtaining the leaf node corresponding to the identity information to be verified and leaf nodes of a according to a mapping relationship between a category of the identity information to be verified and a leaf node of a first Merkle tree and obtaining, from the first Merkle tree, the Merkle proof of the leaf node corresponding to the identity information to be verified, wherein the first Merkle tree is constructed based on a plurality of pieces of identity information of a user; by using a hash algorithm, wherein leaf nodes of the first Merkle

tree encode respective pieces of the plurality of pieces of identity information of the user using the hash algorithm, and

2) a root value of the first Merkle tree; ~~constructed based on the plurality of pieces of identity information of the user, wherein the first Merkle tree is constructed based on the plurality of pieces of identity information of the user using a non hash algorithm and leaf nodes of the first Merkle tree encode, using the non hash algorithm, identity information of the user and other data information, wherein the other data information is a random number and wherein the method further comprises obtaining 3) mapping relationship between the other data information and the leaf nodes of the~~
5
10 first Merkle tree from the storage terminal;

calculating a root value of a second Merkle tree corresponding to the identity information to be verified based on the identity information to be verified; and the other data information and the Merkle proof of the leaf node corresponding to the identity information to be verified; and

15 determining whether the root value of the second Merkle tree ~~corresponding to the identity information to be verified~~ is the same as the root value of the first Merkle tree, ~~constructed based on the plurality of pieces of identity information of the user,~~ wherein, when it is determined that the root value of the second Merkle tree is the same as the root value of the first Merkle tree, the identity information to be verified
20 passes verification and is identity information accepted by the authority;

wherein the storage terminal comprises a server of a certification authority that stores the root value of the first Merkle tree in a digital certificate of the user, wherein the digital certificate comprises a content portion and a signature portion, the content portion comprises the root value of the first Merkle tree and the signature portion is an
25 electronic signature of the content portion, wherein the obtaining, from the storage terminal, the root value of the first Merkle tree comprises:

obtaining the digital certificate of the user;

verifying the digital certificate by using a corresponding public key of the certification authority of the digital certificate; and

30 obtaining the root value of the first Merkle tree after the verification of the digital certificate is passed,

wherein the storage terminal further comprises a blockchain-based distributed database which stores mapping relationships between the plurality of pieces of identity information of the user and the leaf nodes of the first Merkle tree, and the

Merkle proofs of the leaf nodes corresponding to the plurality of pieces of identity information of the user on the first Merkle tree.

2. The method according to claim 1, wherein calculating the root value of the second Merkle tree corresponding to the identity information to be verified based on the identity information to be verified and the Merkle proof of the leaf node corresponding to the identity information to be verified comprises:

performing encoding calculation based on the identity information to be verified to obtain a data digest corresponding to the identity information to be verified, where the data digest is used as a value of a leaf node of the second Merkle tree, and then sequentially performing encoding calculation based on the data digest and a value of each node included in the Merkle proof of the leaf node corresponding to the identity information to be verified, to finally obtain the root value of the second Merkle tree.

3. The method according to claim 1, wherein obtaining, from the storage terminal, the Merkle proof of the leaf node corresponding to the identity information to be verified comprises obtaining, from the blockchain-based distributed database, the Merkle proof of the leaf node corresponding to the identity information to be verified on the first Merkle tree.

~~10. The method according to claim 9, wherein the non-hash algorithm is base 64.~~

~~11. The method according to claim 9 to 10, the storage terminal comprises one or more of a client device of the user, a server of a certification authority, or a blockchain-based distributed database.~~

~~12. The method according to claim 11, the storage terminal comprises the server of the certification authority;~~

~~the root value of the first Merkle tree constructed based on the plurality of pieces of identity information of the user is stored by the certification authority in a digital certificate of the user, wherein the digital certificate comprises a content portion and a signature portion, the content portion comprises the root value of the first Merkle tree constructed based on the plurality of pieces of identity information of the user, and the~~

~~signature portion is an electronic signature of the content portion; and~~

~~obtaining, from the storage terminal, the root value of the first Merkle tree constructed based on the plurality of pieces of identity information of the user comprises:~~

5 ~~obtaining the digital certificate of the user;~~

~~verifying the digital certificate by using a corresponding public key of the certification authority of the digital certificate; and~~

~~obtaining the root value of the first Merkle tree constructed based on the plurality of pieces of identity information of the user after verification is passed.~~

10

~~13. The method according to claim 12, wherein the content portion of the digital certificate further comprises the mapping relationships between the plurality of pieces of identity information of the user and the leaf nodes of the first Merkle tree, and Merkle proofs of the leaf nodes corresponding to the plurality of pieces of identity information of the user on the first Merkle tree constructed based on the plurality of pieces of identity information of the user; and~~

15

~~obtaining, from the storage terminal, the Merkle proof of the leaf node corresponding to the identity information to be verified on the first Merkle tree constructed based on the plurality of pieces of identity information of the user comprises:~~

20

~~obtaining the digital certificate of the user;~~

~~verifying the digital certificate by using the corresponding public key of the certification authority of the digital certificate; and~~

~~obtaining a mapping relationship between the identity information to be verified and the leaf node after the verification is passed, and obtaining, based on the mapping relationship between the identity information to be verified and the leaf node, the Merkle proof of the leaf node corresponding to the identity information to be verified on the first Merkle tree constructed based on the plurality of pieces of identity information of the user.~~

25
30

~~14. The method according to claim 13, wherein the storage terminal further comprises the client device of the user or a blockchain-based distributed database, and the mapping relationships between the plurality of pieces of identity information of the user and the Merkle proofs of the leaf nodes corresponding to the plurality of~~

~~pieces of identity information of the user on the first Merkle tree constructed based on the plurality of pieces of identity information of the user are stored in the client device of the user or the blockchain-based distributed database.~~

5 ~~15.4.~~ The method according to claim ~~13~~1, wherein the content portion of the digital certificate of the user further comprises a public key of the user.

10 ~~16.5.~~ The method according to claim ~~9~~1, wherein the plurality of pieces of identity information of the user comprises one or more of a public key of the user, a name of the user, an address of the user, or an identification number of the user.

15 ~~17.6.~~ A computer device, comprising a storage device and a processor, wherein the storage device stores a computer program that can be run by the processor;; wherein the computer program, when run by the processor, causes the processor to perform ~~the a~~ method according to any one of ~~claims 1 to 16~~the preceding claims.

20 ~~18.7.~~ A computer-readable storage medium storing a computer program which, when executed by a computing device, causes the computing device to perform the method according to ~~any one of claim 1 or~~ any one of claims 1 to ~~16~~5.