

CLAIMS

What is claimed is:

1. An identify information authentication method, comprising:

obtaining a plurality of pieces of identity information of a user;

5 constructing 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 identity information of the user; and

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
10 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, and a root value of the Merkle tree constructed based on the plurality of pieces of identity information of the user.

2. The method according to claim 1, wherein the leaf nodes of the Merkle tree
15 are encoded based on the identity information of the user and other data information; and

the method further comprises: transmitting mapping relationships between the other data information and the leaf nodes to the storage terminal.

3. The method according to claim 2, wherein the other data information is a
20 random number.

4. The method according to any one of claims 1 to 3, wherein the storage terminal comprises one or more of a client device of a user, a server of a certification authority, or a blockchain-based distributed database.

5. The method according to any one of claims 1 to 3, wherein the storage
25 terminal comprises a server of a 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.

6. The method according to claim 5, 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.

7. The method according to claim 5, wherein the storage terminal further comprises a client device of a 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.

8. 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.

9. 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.

10. The method according to any one of claims 1 to 3, wherein the encoding comprises hash encoding.

11. An identify information verification method, comprising:
in response to identity information to be verified, obtaining, from a storage terminal, a Merkle proof of a leaf node corresponding to the identity information to be verified based on mapping relationships between the identity information to be verified and leaf nodes of a Merkle tree constructed based on a plurality of pieces of identity information of a user, and a root value of the Merkle tree constructed based on the plurality of pieces of identity information of the user, wherein leaf nodes of the Merkle tree are generated by encoding identity information of the user;

calculating a root value of a Merkle tree corresponding to the identity information to be verified based on the identity information to be verified and the Merkle proof; and

determining whether the root value of the Merkle tree corresponding to the identity information to be verified is the same as the root value of the Merkle tree constructed based on the plurality of pieces of identity information of the user.

12. The method according to claim 11, wherein the leaf nodes of the Merkle tree

are encoded based on the identity information of the user and other data information;
and

the method further comprises: obtaining mapping relationships between the other data information and the leaf nodes from the storage terminal; and

5 calculating a root value of a Merkle tree corresponding to the identity information to be verified based on the identity information to be verified and the Merkle proof comprises:

calculating the root value of the Merkle tree corresponding to the identity information to be verified based on the identity information to be verified, the other
10 data information, and the Merkle proof.

13. The method according to claim 12, wherein the other data information is a random number.

14. The method according to any one of claims 11 to 13, the storage terminal comprises one or more of a client device of a user, a server of a certification authority,
15 or a blockchain-based distributed database.

15. The method according to any one of claims 11 to 13, the storage terminal comprises a server of a certification authority.

the root value of the Merkle tree constructed based on the plurality of pieces of identity information of the user is stored by the certification authority in a digital
20 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 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 Merkle tree
25 constructed based on the plurality of pieces of identity information of the user comprises:

obtaining a digital certificate of the user;

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

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

16. The method according to claim 15, 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; and

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

obtaining a digital certificate of the user;

verifying the digital certificate by using a corresponding public key of a 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 Merkle tree constructed based on the plurality of pieces of identity information of the user.

17. The method according to claim 15, wherein the storage terminal further comprises a client device of a 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.

18. The method according to claim 15, wherein the content portion of the digital certificate of the user further comprises a public key of the user.

19. The method according to claim 11, 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.

20. The method according to any one of claims 11 to 13, wherein the encoding comprises hash encoding.

21. An identity information authentication device comprising a plurality of units configured to perform the method of any one of claims 1-8, wherein the plurality of units comprise an acquisition unit, a Merkle tree construction unit, and a transmitting unit.

22. An identity information verification device comprising a plurality of units

configured to perform the method of any one of claims 11-18, wherein the plurality of units comprise an acquisition unit, a calculation unit, and a comparing unit.

23. A computer device, comprising a storage device and a processor, wherein the storage device stores a computer program that can be run by a processor; and when
5 the processor runs the computer program, the method according to any one of claims 1 to 10 is performed.

24. A computer device, comprising a storage device and a processor, wherein the storage device stores a computer program that can be run by a processor; and when
the processor runs the computer program, the method according to any one of claims
10 11 to 20 is performed.

25. A computer-readable storage medium, wherein the medium stores computer programs, and when the computer programs are executed by a processor, the method according to any one of claims 1 to 10 is performed.

26. A computer-readable storage medium, wherein the medium stores computer
15 programs, and when the computer programs are executed by a processor, the method according to any one of claims 11 to 20 is performed.