

CLAIMS

What is claimed is:

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

5 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, comprising obtaining the leaf node corresponding to the identity information to be verified according to a mapping relationship between a category of the identity
10 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
15 identity information of the user using the hash algorithm, and

2) a root value of the first Merkle tree;

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 Merkle proof of the leaf node corresponding to the identity information to be verified;

20 and

determining whether the root value of the second Merkle tree is the same as the root value of the first Merkle tree, 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 passes verification and is identity information
25 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
30 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

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
5 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.

10 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
15 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.

20 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
25 verified on the first Merkle tree.

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

30 5. The method according to claim 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.

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 a method according to any one of the preceding claims.

- 5 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 claims 1 to 5.