

USER IDENTITY INFORMATION AUTHENTICATION AND VERIFICATION METHODS AND DEVICES

ABSTRACT

5 One or more embodiments of the present application provide user identity
information authentication and verification methods and devices. The user identity
information authentication method includes: obtaining a plurality of pieces of identity
information of a user; constructing a Merkle tree based on the plurality of pieces of
10 identity information of the user, where 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 leaf nodes corresponding to the plurality
of pieces of identity information of the user on the Merkle tree constructed based on
15 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. The storage terminal can include one or more of a client device of a user, a
server of a certification authority, or a blockchain-based distributed database.

FIG. 1