

CLAIMS:

1. A computer-implemented method for decentralized-identifier creation, comprising:
receiving a request for obtaining a decentralized identifier (DID), wherein the request comprises an account identifier;

obtaining, in response to receiving the request, a public key of a cryptographic key pair;

obtaining the DID based on the public key; and

storing a mapping relationship between the account identifier and the obtained DID.

2. The method of claim 1, wherein the receiving a request for obtaining a DID comprises:

receiving the request from a first entity on behalf of a second entity for creating the DID for the second entity, wherein the account identifier corresponds to the second entity.

3. The method of claim 2, further comprising:

determining an existing DID associated with the first entity based on the request.

4. The method of any of the claims 2-3, further comprising:

determining that the request comprises a proof of real-name authentication of the second entity.

5. The method of any of the preceding claims, wherein the request comprises an application programming interface (API) message.

6. The method of any of the preceding claims, wherein the obtaining a public key of a cryptographic key pair comprises:

sending a request to a key management system (KMS) for generating and storing the cryptographic key pair; and

receiving the public key of the cryptographic key pair from the KMS.

7. The method of any of the preceding claims, wherein the obtaining a DID comprises:

generating a blockchain transaction for creating a blockchain account, wherein the obtained DID comprises a blockchain address associated with the blockchain account.

8. The method of any of the preceding claims, wherein the obtaining a DID comprises:
generating, based on the public key, one or more blockchain transactions for creating the DID and adding a DID document associated with the DID to a blockchain.

9. The method of claim 8, wherein the one or more blockchain transactions invoke one or more blockchain contracts associated with the blockchain.

10. The method of any of the claims 8-9, wherein the DID document comprises:
one or more public keys associated with the obtained DID;
authentication information associated with the obtained DID;
authorization information associated with the obtained DID;
delegation information associated with the obtained DID;
one or more services associated with the obtained DID;
one or more service endpoints associated with the obtained DID; or
a DID of a creator of the obtained DID.

11. The method of any of the claims 8-10, wherein the DID document comprises:
the mapping relationship between the account identifier and the obtained DID.

12. The method of claim 11, wherein the mapping relationship in the DID document is encrypted.

13. The method of any of the preceding claims, wherein the obtaining a DID comprises:

sending a request to a KMS for signing a blockchain transaction using a private key of the cryptographic key pair; and

receiving from the KMS a signed version of the blockchain transaction, wherein the signed version of the blockchain transaction is generated in a Trusted Execution Environment (TEE).

14. The method of any of the preceding claims, further comprising:

receiving a request associated with the obtained DID, wherein the request comprises the account identifier; and

identifying the obtained DID based on the mapping relationship between the account identifier and the obtained DID.

15. The method of claim 13, further comprising:
storing a recovery key associated with the obtained DID.

16. A system for decentralized-identifier creation, comprising:
one or more processors; and
one or more computer-readable memories coupled to the one or more processors and having instructions stored thereon that are executable by the one or more processors to perform the method of any of claims 1 to 15.

17. A non-transitory computer-readable storage medium configured with instructions executable by one or more processors to cause the one or more processors to perform the method of any of claims 1 to 15.

18. An apparatus for decentralized-identifier creation comprising a plurality of modules for performing the method of any of claims 1 to 15.