

CLAIMS

1. A computer-implemented method for blockchain-based decentralized-identifier creation, comprising:

obtaining a request for creating a decentralized identifier (DID), wherein the request comprises a public key of a cryptographic key pair;

creating, based on the public key, a blockchain account associated with a blockchain;

creating the DID based on information associated with the blockchain account; and

returning a confirmation message comprising the created DID.

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

receiving the request from a computing device associated with a first entity for creating the DID on behalf of a second entity.

3. The method of claim 2, wherein the request for creating the DID further comprises:

an account identifier associated with the second entity;

profile information associated with the second entity;

information about one or more services associated with the DID; or

a callback address associated with the first entity or the second entity.

4. The method of claim 3, further comprising:

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

5. The method of any of the preceding claims, wherein:

the request for creating the DID comprises an application programming interface (API) message.

6. The method of any of the preceding claims, wherein the creating the DID comprises:

determining that the DID is not duplicative of any existing DID associated with the blockchain.

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

obtaining a DID document corresponding to the DID.

8. The method of claim 7, wherein the DID document comprises:

the public key;

authentication information associated with the created DID;

authorization information associated with the created DID;

delegation information associated with the created DID;

one or more services associated with the created DID; or

one or more service endpoints associated with the created DID.

9. The method of any of claims 7 to 8, further comprising:

generating a blockchain transaction for adding the DID document to the blockchain;

and

sending the generated blockchain transaction to one or more blockchain nodes associated with the blockchain for adding to the blockchain.

10. The method of claim 9, wherein:

the blockchain transaction invokes a blockchain contract for managing relationships between DIDs and corresponding DID documents; and

the blockchain contract is associated with the blockchain.

11. The method of claim 10, wherein:

the blockchain contract comprises an interface for adding one or more DID documents to the blockchain.

12. The method of any of claims 9 to 11, wherein the generating a blockchain transaction for adding the DID document to the blockchain comprises:

generating an unsigned blockchain transaction for adding the DID document to the blockchain;

determining a hash value of the unsigned blockchain transaction;

sending the hash value to a computing device associated with a sender of the request for creating the DID;

receiving a digital signature from the computing device associated with the sender of the request for creating the DID, wherein the digital signature is generated by encrypting the hash value using a private key of the cryptographic key pair; and

adding the digital signature to the unsigned blockchain transaction to generate the blockchain transaction for adding the DID document to the blockchain.

13. The method of claim 12, wherein the generating the unsigned blockchain transaction comprises including one or more information items in the unsigned blockchain transaction, the one or more information items comprising:

an address associated with the blockchain;

an identifier of a blockchain contract associated with the unsigned blockchain transaction;

version information of the blockchain contract associated with the unsigned blockchain transaction; or

information of one or more interfaces of the blockchain contract associated with the unsigned blockchain transaction.

14. 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 13.

15. 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 13.

16. An apparatus for decentralized-identifier creation comprising a plurality of modules for performing the method of any of claims 1 to 13.