

CLAIMS

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

obtaining a request for authenticating a decentralized identifier (DID), wherein the request comprises the DID, a plaintext associated with a challenge for authenticating the DID, and a digital signature on the plaintext;

obtaining a public key associated with the DID;

determining, based on the obtained public key and the plaintext, that the digital signature on the plaintext is created based on a private key corresponding to the DID; and

generating, based on the determination, a message confirming authentication of the DID.

2. The method of claim 1, wherein the obtaining a public key associated with the DID comprises:

identifying a blockchain associated with the DID; and

obtaining the public key from the identified blockchain.

3. The method of claim 2, wherein the obtaining the public key from the identified blockchain comprises:

sending a blockchain transaction to one or more blockchain nodes of the blockchain to retrieve a DID document corresponding to the DID, wherein the blockchain transaction comprises information associated with the DID;

obtaining the DID document from the blockchain; and

retrieving the public key from the DID document.

4. The method of claim 3, wherein the blockchain transaction invokes a blockchain contract for managing relationships between DIDs and corresponding DID documents.

5. The method of claim 4, wherein the blockchain contract comprises an interface for retrieving information associated with one or more DID documents corresponding to one or more DIDs.

6. The method of any of claims 1 to 5, further comprising:

sending the message confirming authentication of the DID to a computing device associated with a creator of the challenge for authenticating the DID; or

sending the message confirming authentication of the DID to a computing device associated with a sender of the request for authenticating the DID for the sender to forward the message to the creator of the challenge.

7. The method of any of claims 1 to 6, wherein the obtained request for authenticating the DID comprises:

a response to the challenge for authenticating the DID, the response comprising the digital signature on the plaintext.

8. The method of any of claims 1 to 7, further comprising, prior to obtaining the request for authenticating the DID:

obtaining a request for creating the digital signature, wherein the request for creating the digital signature comprises the plaintext and information associated with the DID; and

creating the digital signature on the plaintext based on the request for creating the digital signature.

9. The method of claim 8, wherein the creating the digital signature on the plaintext comprises:

obtaining one or more permissions associated with a sender of the request for creating the digital signature;

determining, based on the obtained one or more permissions and the information associated with the DID, whether the sender of the request for creating the digital signature is authorized to control one or more operations associated with the DID; and

in response to determining that the sender of the request for creating the digital signature is authorized to control the one or more operations associated with the DID, creating the digital signature on the plaintext.

10. The method of claim 9, wherein the sender of the request for creating the digital signature comprises:

an owner of the DID; or

an entity authorized to control the one or more operations associated with the DID on behalf of the owner of the DID.

11. The method of any of claims 8 to 10, wherein the creating the digital signature on the plaintext comprises:

 sending instructions to a key management system (KMS) for signing the plaintext using the private key associated with the DID; and
 obtaining the digital signature from the KMS.

12. The method of claim 11, wherein the sending instructions to the KMS comprises:
 identifying a blockchain account associated with the DID;
 determining an identifier for the private key associated with the DID based on the identified blockchain account associated with the DID; and
 including the identifier for the private key associated with the DID in the instructions.

13. The method of any of claims 11 to 12, wherein the private key is stored in a trusted execution environment (TEE) associated with the KMS and the digital signature obtained from the KMS is generated in the TEE.

14. A system for decentralized-identifier authentication, 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. An apparatus for decentralized-identifier authentication comprising a plurality of modules for performing the method of any of claims 1 to 13.

16. 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.