

CLAIMS

1. A computer-implemented method for blockchain-based cross-entity authentication, comprising:

obtaining, from a blockchain, a blockchain transaction comprising an authentication request by a first entity for authenticating a user, wherein the authentication request comprises a decentralized identifier (DID) of the user;

in response to determining that the first entity is permitted to access authentication information of the user endorsed by a second entity, obtaining an authentication result of the user by the second entity in response to the obtained blockchain transaction, wherein the authentication result is associated with the DID;

generating a different blockchain transaction comprising the authentication result; and

transmitting the different blockchain transaction to a blockchain node for adding to the blockchain.

2. The method of claim 1, before obtaining the blockchain transaction, further comprising:

obtaining the authentication request by the first entity for authenticating a user;

generating the blockchain transaction for obtaining the authentication result of the user by the second entity; and

transmitting the blockchain transaction to a blockchain node for adding to the blockchain.

3. The method of any of claims 1-2, further comprising:

obtaining the different blockchain transaction from the blockchain, the different blockchain transaction comprising the authentication result of the user by the second entity, wherein the authentication result indicates that the authentication succeeded; and

transmitting the authentication result to the first entity for granting the user access to the first entity.

4. The method of any of claims 1-2, further comprising:

obtaining the different blockchain transaction from the blockchain, the different blockchain transaction comprising the authentication result of the user by the second entity, wherein the authentication result indicates that the authentication failed; and

transmitting the authentication result to the first entity for denying the user access to the first entity.

5. The method of any of claims 1-4, wherein:
the user is registered with the second entity; and
the user is not registered with the first entity.

6. The method of any of claims 1-5, wherein:
the obtained blockchain transaction comprises an authorization encrypted with a private key of the user for permitting the first entity to access the authentication information of the user endorsed by the second entity;

the encrypted authorization comprises the DID of the user;

the encrypted authorization comprises a digital signature on the authentication request based on a private key of the first entity; and

after obtaining the blockchain transaction and before obtaining the authentication result, the method further comprises:

obtaining a public key of the user;

decrypting the encrypted authorization with the public key of the user to verify that the authorization is signed by the user and to obtain the digital signature;

obtaining a public key of the first entity from the blockchain;

decrypting the digital signature with the obtained public key of the first entity;

and

comparing the decrypted digital signature with a hash value of the authentication request to verify that the authentication request is signed by the first entity.

7. The method of any of claims 1-6, wherein:

the authentication information of the user endorsed by the second entity comprises information associated with a verifiable claim (VC) indicating that the user is a registered user of the second entity; and

the VC is associated with the DID.

8. The method of claim 7, wherein:

the VC comprises a permission configured by the second entity or the user for permitting the first entity to access the VC; and

after obtaining the blockchain transaction and before obtaining the authentication result, the method further comprises: verifying based on the permission that the first entity is permitted to access the VC.

9. The method of any of claims 7-8, wherein:

a hash value of the VC is stored in the blockchain;

the VC is stored in a data store; and

the data store comprises one or more of the following: a local data store maintained by the second entity, a public data store accessible to the second entity, and a data store maintained by a platform for the second entity.

10. The method of claim 9, wherein obtaining the authentication result in response to the obtained blockchain transaction comprises:

querying the data store to obtain the VC associated with the DID;

verifying whether the user is the registered user of the second entity based on the obtained VC to generate an unencrypted authentication result; and

encrypting the unencrypted authentication result with a private key of the second entity to generate the authentication result.

11. The method of any of claims 7-10, before obtaining the blockchain transaction, further comprising:

obtaining, from a computing device associated with the second entity, a VC creation request for creating the VC indicating that the user is a registered user of the second entity;

obtaining a digital signature associated with the second entity; and

creating the VC based on the obtained VC creation request and the obtained digital signature.

12. The method of claim 11, before obtaining the VC creation request, further comprising:

obtaining, from the second entity, a DID creation request for creating the DID associated with an account identifier of the user;

obtaining 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.

13. The method of any of claims 1-12, wherein:

the DID is a secondary DID associated with a primary DID of the user;

the primary DID is associated with privacy information of the user; and

the privacy information is untraceable based on the secondary DID.

14. The method of claim 13, wherein:

the secondary DID is a temporary DID for the user to access the first entity.

15. A system for blockchain-based cross-entity 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 14.

16. An apparatus for blockchain-based cross-entity authentication comprising a plurality of modules for performing the method of any of claims 1 to 14.

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 14.