

CLAIMS

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

obtaining 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, generating a blockchain transaction for obtaining an authentication result of the user by the second entity, wherein the authentication result is associated with the DID; and

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

2. The method of claim 1, further comprising:

obtaining, from the blockchain, the blockchain transaction for obtaining the authentication result of the user;

obtaining an authentication result associated with the DID in response to the obtained blockchain transaction;

generating a different blockchain transaction comprising the authentication result; and

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

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

obtaining a 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 a 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 claim any of claims 1-5, wherein before generating the blockchain transaction for obtaining the authentication result of the user by the second entity, the method further comprises:

obtaining a public key of the user from the blockchain based on the DID; and
verifying that the user owns the DID based at least on the obtained public key of the user.

7. The method of claim 6, wherein:

before generating the blockchain transaction for obtaining the authentication result of the user by the second entity, the method further comprises:

generating a digital signature on the obtained authentication request with a private key of the first entity, and

obtaining 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 digital signature;

the encrypted authorization comprises the DID of the user; and

the generated blockchain transaction comprises the encrypted authorization.

8. The method of any of claims 1-7, 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.

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

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

11. The method of any of claims 1-10, 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.

12. The method of claim 11, wherein:

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

13. 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 12.

14. An apparatus for blockchain-based cross-entity authentication comprising a plurality of modules for performing the method of any of claims 1 to 12.

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 12.