

SYSTEM AND METHOD FOR BLOCKCHAIN-BASED CROSS-ENTITY AUTHENTICATION

CROSS REFERENCE TO RELATED APPLICATIONS

[1] This application claims priority to and benefits of International Application No. PCT/CN2019/095299, filed with the China National Intellectual Property Administration (CNIPA) on July 9, 2019, International Application No. PCT/CN2019/095303, filed with the CNIPA on July 9, 2019, and International Application No. PCT/CN2019/094396, filed with the CNIPA on July 2, 2019. Both of International Application No. PCT/CN2019/095299 and International Application No. PCT/CN2019/095303 claim priority to and benefits of International Application No. PCT/CN2019/094396. The entire contents of all of the above-identified applications are incorporated herein by reference.

TECHNICAL FIELD

[2] This application generally relates to methods and devices for blockchain-based cross-entity authentication.

BACKGROUND

[3] Traditional identity management systems are based on centralized authorities such as corporate directory services, certificate authorities, or domain name registries. Each of the centralized authorities may serve as a root of trust that provides credibility to the identity it endorses. For such systems, data associated with the identities is often stored in centralized databases, if not traditional information storage media. The maintenance of identity of each person or entity is under the control of the centralized authorities. Given its nature, traditional identity management systems are subject to security risks suffered by each of the centralized authorities and provide inefficient mechanisms for the aggregation of identities or credentials provided by different centralized authorities. In such systems, individual entities or identity owners are often neither free to choose the root of trust nor in control over their own identities or credentials. Authentication and verification of their identities often prove to be inefficient.

[4] Cross-entity authentication presents additional challenges. Cross-entity authentication requires different authorities to share user identity information. For example, to allow a first authority to authenticate a user based on the user's registration with a second authority, the second authority may need to share the user's identity and authentication

CLAIMS

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

obtaining, at a first computing system from a first entity, an authentication request for authenticating a user, wherein the authentication request comprises a decentralized identifier (DID) of the user;

determining, at the first computing system, that the first entity is permitted to access authentication information of the user corresponding to the DID, wherein the authentication information is endorsed by a second entity;

generating, at the first computing system, a blockchain transaction for obtaining an authentication result endorsed by the second entity of whether the DID is registered with the second entity;

adding the blockchain transaction to a blockchain;

obtaining, at the first computing system, a different blockchain transaction from the blockchain, the different blockchain transaction comprising the authentication result endorsed by the second entity of whether the DID is registered with the second entity; and

transmitting the obtained authentication result to the first entity for granting or denying the user access to the first entity based on the obtained authentication result.

2. The method of claim 1, after adding the blockchain transaction to the blockchain and before obtaining the different blockchain transaction, further comprising:

obtaining, at a second computing system from the blockchain, the blockchain transaction for obtaining the authentication result;

obtaining, at the second computing system, the authentication result by searching for the authentication information corresponding to the DID in a data store in response to the obtained blockchain transaction for obtaining the authentication result;

generating, at the second computing system, the different blockchain transaction comprising the authentication result; and

adding the different blockchain transaction to the blockchain.

3. The method of claim 1, wherein:

the authentication result indicates that the DID is registered with the second entity; and

transmitting the obtained authentication result to the first entity for granting or denying the user access to the first entity based on the obtained authentication result comprises transmitting the obtained authentication result to the first entity for granting the user access to the first entity.

4. The method of claim 1, wherein:

the authentication result indicates that the DID is not registered with the second entity; and
transmitting the obtained authentication result to the first entity for granting or denying the user access to the first entity based on the obtained authentication result comprises transmitting the obtained authentication result to the first entity for denying the user access to the first entity.

6. The method of claim 1, wherein before generating the blockchain transaction for obtaining the authentication result, the method further comprises:

obtaining, at the first computing system, a public key of the user from the blockchain based on the DID; and

verifying, at the first computing system, 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, the method further comprises:

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

generating, at the first computing system, an authorization encrypted with a private key of the user indicating a permission for 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.

11. The method of claim 1, wherein:

the DID comprises a secondary DID;

the user corresponds to a primary DID and the secondary DID both known by the second entity;

the primary DID corresponds to privacy information of the user that is untraceable based on the secondary DID; and

the secondary DID is a limited-use DID for the user to access the first entity.

12. The method of claim 11, wherein:

the limited-use DID is limited by an expiring time, limited by an expiring number of use, or limited for accessing only the first entity.

13. A system for blockchain-based cross-entity authentication, the system comprising one or more processors and one or more non-transitory computer-readable memories coupled to the one or more processors and configured with instructions executable by the one or more processors to cause the system to perform operations comprising:

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

determining that the first entity is permitted to access authentication information of the user corresponding to the DID, wherein the authentication information is endorsed by a second entity;

generating a blockchain transaction for obtaining an authentication result endorsed by the second entity of whether the DID is registered with the second entity;

adding the blockchain transaction to a blockchain;

obtaining a different blockchain transaction from the blockchain, the different blockchain transaction comprising the authentication result endorsed by the second entity of whether the DID is registered with the second entity; and

transmitting the obtained authentication result to the first entity for granting or denying the user access to the first entity based on the obtained authentication result.

14. The system of claim 13, 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.

15. The system of claim 13, wherein:

the authentication result indicates that the DID is registered with the second entity; and

the operations further comprise transmitting the obtained authentication result to the first entity for granting or denying the user access to the first entity based on the obtained

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

16. The system of claim 13, wherein:

the authentication result indicates that the DID is not registered with the second entity;
and

the operations further comprise transmitting the obtained authentication result to the first entity for granting or denying the user access to the first entity based on the obtained authentication result comprises transmitting the obtained authentication result to the first entity for denying the user access to the first entity.

17. A non-transitory computer-readable storage medium for blockchain-based cross-entity authentication, the storage medium configured with instructions executable by one or more processors to cause the one or more processors to perform operations comprising:

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

determining that the first entity is permitted to access authentication information of the user corresponding to the DID, wherein the authentication information is endorsed by a second entity;

generating a blockchain transaction for obtaining an authentication result endorsed by the second entity of whether the DID is registered with the second entity;

adding the blockchain transaction to a blockchain;

obtaining a different blockchain transaction from the blockchain, the different blockchain transaction comprising the authentication result endorsed by the second entity of whether the DID is registered with the second entity; and

transmitting the obtained authentication result to the first entity for granting or denying the user access to the first entity based on the obtained authentication result.

18. The storage medium of claim 17, 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.

19. The storage medium of claim 17, wherein:

the authentication result indicates that the DID is registered with the second entity; and
the operations further comprise transmitting the obtained authentication result to the first entity for granting or denying the user access to the first entity based on the obtained authentication result comprises transmitting the obtained authentication result to the first entity for granting the user access to the first entity.

20. The storage medium of claim 17, wherein:
the authentication result indicates that the DID is not registered with the second entity; and
the operations further comprise transmitting the obtained authentication result to the first entity for granting or denying the user access to the first entity based on the obtained authentication result comprises transmitting the obtained authentication result to the first entity for denying the user access to the first entity.