

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/CN2019/094936, 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, from a blockchain, a blockchain transaction comprising an authentication request by a first entity for authenticating a user, wherein the user corresponds to a primary DID (decentralized identifier) and a secondary DID both known by a second entity, the primary DID corresponds to privacy information of the user that is untraceable based on the secondary DID, the secondary DID is a limited-use DID for the user to access the first entity, and the authentication request comprises the secondary DID;

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

obtaining, at the second entity, an authentication result of whether the user is registered with the second entity by searching for the authentication information corresponding to the primary DID in a data store;

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

3. The method of claim 1, further comprising:

obtaining the different blockchain transaction from the blockchain, the different blockchain transaction comprising the authentication result, 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 claim 1, further comprising:

obtaining the different blockchain transaction from the blockchain, the different blockchain transaction comprising the authentication result, 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 claim 1, wherein:

the user is registered with the second entity; and

the user is not registered with the first entity.

6. The method of claim 1, 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 secondary 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 claim 1, wherein:

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

the VC corresponds to the primary 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 claim 7, wherein:

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

the VC is stored in the 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 comprises:

querying the data store to obtain the VC corresponding to the primary 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 claim 7, before obtaining the blockchain transaction, further comprising:

obtaining, from a computing device corresponding to 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 corresponding to 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 primary DID corresponding to an account identifier of the user;

obtaining a public key of a cryptographic key pair;

obtaining the primary DID based on the public key; and

storing a mapping relationship between the account identifier and the obtained primary DID.

13. The method of claim 1, wherein:

the limited-use DID is limited by an expiring time or an expiring number of use.

14. The method of claim 1, wherein:

the secondary DID is limited for accessing only the first entity.

15. 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 blockchain, a blockchain transaction comprising an authentication request by a first entity for authenticating a user, wherein the user corresponds to a primary DID (decentralized identifier) and a secondary DID both known by a second entity, the primary DID corresponds to privacy information of the user that is untraceable based on the secondary DID, the secondary DID is a limited-use DID for the user to access the first entity, and the authentication request comprises the secondary DID;

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

obtaining, at the second entity, an authentication result of whether the user is registered with the second entity by searching for the authentication information corresponding to the primary DID in a data store;

generating a different blockchain transaction comprising the authentication result; and
transmitting the different blockchain transaction to a blockchain node for adding to the blockchain.

16. The system of claim 15, wherein the operations further comprise:

obtaining the different blockchain transaction from the blockchain, the different blockchain transaction comprising the authentication result, 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.

17. The system of claim 15, wherein the operations further comprise:

obtaining the different blockchain transaction from the blockchain, the different blockchain transaction comprising the authentication result, 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.

18. 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 blockchain, a blockchain transaction comprising an authentication request by a first entity for authenticating a user, wherein the user corresponds to a primary DID (decentralized identifier) and a secondary DID both known by a second entity, the primary DID corresponds to privacy information of the user that is untraceable based on the secondary DID, the secondary DID is a limited-use DID for the user to access the first entity, and the authentication request comprises the secondary DID;

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

obtaining, at the second entity, an authentication result of whether the user is registered with the second entity by searching for the authentication information corresponding to the primary DID in a data store;

generating a different blockchain transaction comprising the authentication result; and
transmitting the different blockchain transaction to a blockchain node for adding to the blockchain.

19. The storage medium of claim 18, wherein the operations further comprise:

obtaining the different blockchain transaction from the blockchain, the different blockchain transaction comprising the authentication result, 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.

20. The storage medium of claim 18, wherein the operations further comprise:

obtaining the different blockchain transaction from the blockchain, the different blockchain transaction comprising the authentication result, 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.