SYSTEM AND METHOD FOR BLOCKCHAIN-BASED NOTIFICATION

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 notification.

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 for activities such as receiving notifications often prove to be inefficient.

[4] Blockchain technology provides an opportunity to establish a trustworthy decentralized system that does not require trust in each member of the system. Blockchain provides data storage in a decentralized fashion by keeping the data in a series of data blocks having precedence relationship between each other. The chain of blocks is maintained and updated by a network of blockchain nodes, which are also responsible for validating data

CLAIMS

1. A computer-implemented method for blockchain-based notification, comprising:

obtaining, from a computing device associated with a first decentralized identifier (DID), a query about event data;

in response to the obtained query, searching a data store to obtain one or more notifications for event data associated with a second DID, wherein a DID document associated with the second DID comprises the first DID, and wherein the DID document is stored in a blockchain; and

providing the one or more notifications for the computing device associated with the first DID.

2. The method of claim 1, wherein:

the DID document comprises a parameter indicating a creator of the second DID; and

the parameter comprises the first DID.

3. The method of claim 1, wherein:

the DID document comprises a parameter indicating a controller of the second DID; and

the parameter comprises the first DID.

4. The method of claim 1, wherein:

the event data is associated with a verifiable claim; and

a representation of the verifiable claim is stored in the blockchain.

5. The method of claim 1, wherein the event data associated with the second DID comprises one or more of the following:

a registration of the second DID in the blockchain;

an update to the DID document in the blockchain;

an issuance of a first verifiable claim associated with the second DID, wherein the second DID corresponds to an issuer of the first verifiable claim; and

an issuance of a second verifiable claim associated with the second DID, wherein the second DID corresponds to a subject of the second verifiable claim.

6. The method of claim 1, before obtaining the query, further comprising:

obtaining a plurality of notifications from one or more message queues; and

storing the plurality of notifications in the data store in association with information of corresponding DIDs and corresponding blockchain heights in the blockchain, wherein the plurality of notifications comprise the one or more notifications for the event data associated with the second DID.

7. The method of claim 6, after obtaining the plurality of notifications, further comprising:

filtering the plurality of notifications to remove one or more unauthorized notifications.

8. The method of claim 6, after obtaining the plurality of notifications, further comprising:

categorizing the plurality of notifications based on one or more of the following notification parameters: event type, DID, DID creator, DID controller, notification recipient, verifiable claim issuer, and verifiable claim subject.

9. The method of claim 1, wherein searching the data store to obtain the one or more notifications for the event data associated with the second DID comprises:

searching the data store based on a current starting height of the blockchain to obtain the one or more notifications for the event data associated with the second DID.

10. The method of claim 9, wherein:

searching the data store based on the current starting height of the blockchain to obtain the one or more notifications for the event data associated with the second DID comprises: searching from the current starting height of the blockchain to a current ending height of the blockchain for the one or more notifications associated with the event data; and

the method further comprises providing the current ending height of the blockchain for one or more of the following: the computing device associated with the first DID and another computing device associated with the second DID.

11. The method of claim 9, wherein:

the query comprises the current starting height of the blockchain; and

the current starting height of the blockchain comprises an offset from a previous ending height of the blockchain of a previous search.

12. The method of claim 9, wherein:

the query comprises the current starting height of the blockchain; and

the current starting height of the blockchain is a previous ending height of the blockchain of a previous search.

13. A system for blockchain-based notification, 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 computing device associated with a first decentralized identifier (DID), a query about event data;

in response to the obtained query, searching a data store to obtain one or more notifications for event data associated with a second DID, wherein a DID document associated with the second DID comprises the first DID, and wherein the DID document is stored in a blockchain; and

providing the one or more notifications for the computing device associated with the first DID.

14. The system of claim 13, wherein:

the DID document comprises a parameter indicating a creator of the second DID; and

the parameter comprises the first DID.

15. The system of claim 13, wherein:

the DID document comprises a parameter indicating a controller of the second DID; and

the parameter comprises the first DID.

16. The system of claim 13, wherein:

the event data is associated with a verifiable claim; and

a representation of the verifiable claim is stored in the blockchain.

17. A non-transitory computer-readable storage medium for blockchain-based notification, 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 computing device associated with a first decentralized identifier (DID), a query about event data;

in response to the obtained query, searching a data store to obtain one or more notifications for event data associated with a second DID, wherein a DID document associated with the second DID comprises the first DID, and wherein the DID document is stored in a blockchain; and

providing the one or more notifications for the computing device associated with the first DID.

18. The storage medium of claim 17, wherein:

the DID document comprises a parameter indicating a creator of the second DID; and

the parameter comprises the first DID.

19. The storage medium of claim 17, wherein:

the DID document comprises a parameter indicating a controller of the second DID; and

the parameter comprises the first DID.

20. The storage medium of claim 17, wherein:

the event data is associated with a verifiable claim; and

a representation of the verifiable claim is stored in the blockchain.