

unencrypted confirmation document to a third user, referred to as a Relying User, in an attempt to prove the identity of the DID Owner to the Relying User. The Relying User may be, e.g., a service provider or a bank who wants to verify the identity of the DID Owner prior to rendering a service or issuing a loan to the DID Owner. After verification, the Relying User may accept the identity claimed by the DID Owner as true.

[0007] While utilizing such DIDs may allow users to retain control over their own identifiers, doing so may require the DID Owners to have the abilities to store and manage confirmation documents they receive from various Issuers. For example, if a DID Owner has requested multiple confirmation documents from multiple Issuers, the DID Owner may be responsible for storing and managing multiple confirmation documents. Managing multiple confirmation documents may become complicated and time-consuming.

SUMMARY

[0008] In one aspect, a computer-implemented method for providing decentralized identity verification includes: recording an encrypted decentralized identifier (DID) received from a first user; recording a request for confirmation of truthfulness of the encrypted DID, the request being received from a second user; receiving from a third user a response to the request for confirmation and a proof for proving the third user is qualified to respond to the request for confirmation without revealing data used by the third user to generate the response and the proof; recording the response to the request for confirmation; and in response to a determination that the proof is acceptable, indicating the response as valid.

[0009] In another aspect, a device for providing decentralized identity verification includes: 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: record an encrypted decentralized identifier (DID) received from a first user; record a request for confirmation of truthfulness of the encrypted DID, the request being received from a second user; receive from a third user a response to the request for confirmation and a proof for proving the third user is qualified to respond to the request for confirmation; record the response to the request for confirmation without revealing data used by the third user to generate the response and the proof; and in response to a determination that the proof is acceptable, indicate the response as valid.

[0010] In still another aspect, a non-transitory computer-readable medium has stored therein instructions that, when executed by a processor of a device, cause the device to perform a method for providing decentralized identity verification. The method includes: recording an encrypted decentralized identifier (DID) received from a first user; recording a request for confirmation of truthfulness of the encrypted DID, the request being received from a second user; receiving from a third user a response to the request for confirmation and a proof for proving the third user is qualified to respond to the request for confirmation without revealing data used by the third user to generate the response and the proof; recording the response to the request for confirmation; and in response to a determination that the proof is acceptable, indicating the response as valid.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] The accompanying drawings, which are incorporated in and constitute a part of this specification, illustrate embodiments. In the following description, which refers to the drawings, the same numbers in different drawings represent the same or similar elements unless otherwise represented.

What Is Claimed Is:

1. A computer-implemented method for providing decentralized identity verification, the method comprising:

recording an encrypted decentralized identifier (DID) received from a first user;

recording a request for confirmation of truthfulness of the encrypted DID, the request being received from a second user;

receiving from a third user a response to the request for confirmation and a proof for proving the third user is qualified to respond to the request for confirmation without revealing data used by the third user to generate the response and the proof;

recording the response to the request for confirmation; and

in response to a determination that the proof is acceptable, indicating the response as valid.

2. The method of claim 1, wherein the method is performed by one or more nodes in a blockchain system.

3. The method of any preceding claim, further comprising:

reporting an error in response to a determination that the proof is unacceptable.

4. The method of any preceding claim, wherein the proof is a zero-knowledge proof.

5. The method of any preceding claim, further comprising:
providing the response to the second user.
6. The method of any preceding claim, wherein the encrypted DID comprises a plurality of encrypted values corresponding to a plurality of data fields.
7. The method of claim 6, wherein the response to the request for confirmation comprises a truthfulness indicator for each of the plurality of data fields.
8. The method of claim 7, wherein the truthfulness indicator for each particular data field of the plurality of data fields indicates whether or not an encrypted value corresponding to that particular data field is truthful.
9. A device for providing decentralized identity verification, 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 8.
10. An apparatus for providing decentralized identity verification, the apparatus comprising a plurality of modules for performing the method of any of claims 1 to 8.
11. A non-transitory computer-readable medium having stored therein instructions that, when executed by a processor of a device, cause the device to perform the method of any of claims 1 to 8.