CLAIMS

1. A computer-implemented method for blockchain-based decentralized-identifier creation, comprising:

obtaining, by a first computing system from a second computing system, a request for creating a decentralized identifier (DID), wherein the request comprises an account identifier of a user of the second computing system, the account identifier corresponding to a service of the second computing system;

creating, by the first computing system, the DID in response to the request;

sending, by the first computing system to the second computing system, a message comprising the DID;

receiving, by the first computing system from the second computing system, an incomplete blockchain transaction for adding a DID document associated with the DID to a blockchain, the incomplete blockchain transaction comprising the DID document but lacking information associated with the blockchain;

completing, by the first computing system, the incomplete blockchain transaction by adding to the incomplete blockchain transaction an identifier of a blockchain contract invoked by the blockchain transaction;

sending, by the first computing system, the completed blockchain transaction to one or more blockchain nodes associated with the blockchain for adding the completed blockchain transaction to the blockchain;

calculating, by the first computing system, a hash value of a combination of the DID and the account identifier of the user; and

storing, by the first computing system, the hash value as part of the DID document.

2. The method of claim 1, wherein:

the second computing system corresponds to a first entity; and

the request for creating the DID comprises a request by the first entity for creating the DID for the user.

3. The method of claim 2, wherein the request for creating the DID further comprises:

profile information associated with the user;

information about one or more services associated with the DID; or

a callback address associated with the first entity or the user.

4. The method of claim 1, wherein the creating the DID comprises:

determining that the DID is not duplicative of any existing DID associated with the blockchain.

5. The method of claim 1, wherein the DID document comprises:

a public key of a public-private key pair associated with the created DID;

authentication information associated with the created DID;

authorization information associated with the created DID;

delegation information associated with the created DID;

one or more services associated with the created DID; or

one or more service endpoints associated with the created DID.

6. The method of claim 1, wherein the completing the incomplete blockchain transaction further comprises:

adding an address associated with the blockchain to the incomplete blockchain transaction;

adding version information of the blockchain contract to the incomplete blockchain transaction; or

adding to the incomplete blockchain transaction information of an interface for adding one or more DID documents to the blockchain, wherein the blockchain contract comprises one or more interfaces including the interface for adding one or more DID documents to the blockchain.

7. The method of claim 1, wherein the completing the incomplete blockchain transaction further comprises:

determining a hash value of an unsigned version of the blockchain transaction;

sending the hash value of the unsigned version of the blockchain transaction to the second computing system;

receiving a digital signature from the second computing system, wherein the digital signature is generated by encrypting the hash value of the unsigned version of the blockchain transaction using a private key of a cryptographic key pair associated with the DID; and

adding the digital signature to the unsigned version of the blockchain transaction.

8. A non-transitory computer-readable storage medium for blockchain-based decentralized-identifier creation, configured with instructions executable by one or more processors to cause the one or more processors to perform operations comprising:

obtaining, from a computing system, a request for creating a decentralized identifier (DID), wherein the request comprises an account identifier of a user of the computing system, the account identifier corresponding to a service of the computing system;

creating the DID in response to the request;

sending, to the computing system, a message comprising the DID;

receiving, from the computing system, an incomplete blockchain transaction for adding a DID document associated with the DID to a blockchain, the incomplete blockchain transaction comprising the DID document but lacking information associated with the blockchain;

completing the incomplete blockchain transaction by adding to the incomplete blockchain transaction an identifier of a blockchain contract invoked by the blockchain transaction;

sending the completed blockchain transaction to one or more blockchain nodes associated with the blockchain for adding the completed blockchain transaction to the blockchain;

calculating a hash value of a combination of the DID and the account identifier of the user; and

storing the hash value as part of the DID document.

9. The medium of claim 8, wherein:

the computing system corresponds to a first entity; and

the request for creating the DID comprises a request by the first entity for creating the DID for the user.

10. The medium of claim 9, wherein the request for creating the DID further comprises:

profile information associated with the user;

information about one or more services associated with the DID; or

a callback address associated with the first entity or the user.

11. The medium of claim 8, wherein the creating the DID comprises:

determining that the DID is not duplicative of any existing DID associated with the blockchain.

12. The medium of claim8, wherein the DID document comprises:

a public key of a public-private key pair associated with the created DID;

authentication information associated with the created DID;

authorization information associated with the created DID;

delegation information associated with the created DID;

one or more services associated with the created DID; or

one or more service endpoints associated with the created DID.

13. The medium of claim 8, wherein the completing the incomplete blockchain transaction further comprises:

adding an address associated with the blockchain to the incomplete blockchain transaction;

adding version information of the blockchain contract to the incomplete blockchain transaction; or

adding to the incomplete blockchain transaction information of an interface for adding one or more DID documents to the blockchain, wherein the blockchain contract comprises one or more interfaces including the interface for adding one or more DID documents to the blockchain.

14. The medium of claim 8, wherein the completing the incomplete blockchain transaction further comprises:

determining a hash value of an unsigned version of the blockchain transaction;

sending the hash value of the unsigned version of the blockchain transaction to the computing system;

receiving a digital signature from the computing system, wherein the digital signature is generated by encrypting the hash value of the unsigned version of the blockchain transaction using a private key of a cryptographic key pair associated with the DID; and

adding the digital signature to the unsigned version of the blockchain transaction.

15. A system for blockchain-based decentralized-identifier creation, comprising a processor and a non-transitory computer-readable storage medium storing instructions executable by the processor to cause the system to perform operations comprising:

obtaining, from a computing system, a request for creating a decentralized identifier (DID), wherein the request comprises an account identifier of a user of the computing system, the account identifier corresponding to a service of the computing system;

creating the DID in response to the request;

sending, to the computing system, a message comprising the DID;

receiving, from the computing system, an incomplete blockchain transaction for adding a DID document associated with the DID to a blockchain, the incomplete blockchain transaction comprising the DID document but lacking information associated with the blockchain;

completing the incomplete blockchain transaction by adding to the incomplete blockchain transaction an identifier of a blockchain contract invoked by the blockchain transaction;

sending the completed blockchain transaction to one or more blockchain nodes associated with the blockchain for adding the completed blockchain transaction to the blockchain;

calculating a hash value of a combination of the DID and the account identifier of the user; and

storing the hash value as part of the DID document.

16. The system of claim 15, wherein the completing the incomplete blockchain transaction further comprises:

determining a hash value of an unsigned version of the blockchain transaction;

sending the hash value of the unsigned version of the blockchain transaction to the computing system;

receiving a digital signature from the computing system, wherein the digital signature is generated by encrypting the hash value of the unsigned version of the blockchain transaction using a private key of a cryptographic key pair associated with the DID; and

adding the digital signature to the unsigned version of the blockchain transaction.

17. The system of claim 15, wherein:

the computing system corresponds to a first entity; and

the request for creating the DID comprises a request by the first entity for creating the DID for the user.

18. The system of claim 17, wherein the request for creating the DID further comprises:

profile information associated with the user;

information about one or more services associated with the DID; or

a callback address associated with the first entity or the user.

19. The system of claim 15, wherein the creating the DID comprises:

determining that the DID is not duplicative of any existing DID associated with the blockchain.

20. The system of claim 15, wherein the DID document comprises:

a public key of a public-private key pair associated with the created DID;

authentication information associated with the created DID;

authorization information associated with the created DID;

delegation information associated with the created DID;

one or more services associated with the created DID; or

one or more service endpoints associated with the created DID.