CLAIMS

1. An authentication method, comprising:

receiving an authentication request sent from a user, wherein the authentication request comprises an identity identifier of the user;

acquiring authentication data associated with the identity identifier from a blockchain network, wherein a blockchain node of the blockchain network stores a mapping relationship between identity identifiers and authentication data, the authentication data comprises an authentication result, and the authentication result comprises authentication being successful/authentication being failed; and

performing identity authentication on the user according to the authentication data.

2. The authentication method according to claim 1, wherein the method further comprises:

if the authentication request further comprises a public key and a digital signature, verifying whether the digital signature is valid by using the public key, wherein the digital signature is obtained by signing with a private key in the public and private key pair; and

the acquiring authentication data associated with the identity identifier from a blockchain network comprises:

if the verification result indicates that the digital signature is valid, acquiring the authentication data associated with the identity identifier from the blockchain network.

3. The authentication method according to claim 1 or 2, wherein the acquiring authentication data associated with the identity identifier from a blockchain network comprises:

sifting out the authentication data comprising the identity identifier from the blockchain network, and determining the obtained authentication data as the authentication

data associated with the identity identifier.

4. The authentication method according to claim 3, wherein the method further comprises:

if more than one piece of authentication data is obtained after the sifting, determining authentication data satisfying a preset condition in the obtained authentication data, and determining the determined authentication data as the authentication data associated with the identity identifier.

5. The authentication method according to claim 4, wherein the preset condition comprises at least one or more of the following:

a generation time of the authentication data satisfies a preset time condition;

an institution identifier comprised in the authentication data satisfies a preset issuing institution's institution identifier; and

a service type comprised in the authentication data is the same as a service type of a service initiated by the user.

6. The authentication method according to claim 1 or 5, wherein the performing identity authentication on the user according to the authentication data comprises:

determining a current authentication state of the identity identifier according to the authentication data; and

if the identity identifier is in an abnormal state and/or an authentication failed state, determining that the identity authentication on the user is not successful; otherwise, determining that the identity authentication on the user is successful.

7. The authentication method according to claim 6, wherein the method further comprises:

generating authentication data according to the authentication result, wherein the authentication data comprises the identity identifier of the user, an institution identifier of

an institution that generates the authentication result, and the authentication result; and

storing the authentication data to a blockchain node of the blockchain network.

8. The authentication method according to claim 7, wherein before the storing the authentication data to a blockchain node of the blockchain network, the method further comprises:

sending the authentication data to the blockchain network, so that the blockchain network performs consensus processing on the authentication data; and

the storing the authentication data to a blockchain node of the blockchain network comprises:

if the consensus processing result indicates that a consensus is reached, storing the authentication data to a blockchain node of the blockchain network.

9. The authentication method according to claim 6, wherein after the determining that the identity authentication on the user is successful, the method further comprises:

acquiring, according to the service type of the service requested by the user, identity feature information of the user associated with the service type from an identity information management server;

generating authentication data according to the authentication result and the identity feature information, wherein the authentication data comprises the identity identifier of the user, an institution identifier of an institution that generates the authentication result, an authentication event of authenticating the identity feature information, and the authentication result; and

storing the authentication data to a blockchain node of the blockchain network.

10. A blockchain-based authentication data processing method, comprising:

receiving identity information sent from a user, and authenticating the identity information;

generating first authentication data according to the authentication result, wherein the first authentication data comprises the authentication result, an institution identifier of an institution that generates the authentication result, and an identity identifier of the user, and wherein the authentication result comprises authentication being successful/authentication being failed; and

storing the first authentication data to a blockchain node of a blockchain network.

11. The authentication data processing method according to claim 10, wherein the method further comprises:

establishing a mapping relationship between an identity identifier of the user and identity information of the user; and

storing the identity information of the user to an identity information database according to the mapping relationship.

12. The authentication data processing method according to claim 10, wherein the method further comprises:

receiving a loss report or unregistration request sent from the user, wherein the loss report or unregistration request comprises the identity identifier of the user;

determining according to the loss report or unregistration request that the identity information of the user is in an abnormal state;

generating second authentication data according to the identity information of the user being in an abnormal state, the institution identifier of the institution that generates the authentication result, and the identity identifier of the user; and

storing the second authentication data to a blockchain node of the blockchain network.

13. An authentication device, comprising:

a receiving unit configured to receive an authentication request sent from a user, wherein the authentication request comprises an identity identifier of the user;

an acquiring unit configured to acquire authentication data associated with the identity identifier from a blockchain network, wherein a blockchain node of the blockchain network stores a mapping relationship between identity identifiers and authentication data, the authentication data comprises an authentication result, and the authentication result comprises authentication being successful/authentication being failed; and

an authentication unit configured to perform identity authentication on the user according to the authentication data.

14. The authentication device according to claim 13, wherein the authentication device further comprises a verification unit, wherein

the verification unit is configured to, if the authentication request further comprises a public key and a digital signature, verify whether the digital signature is valid by using the public key, wherein the digital signature is obtained by signing with a private key in the public and private key pair; and

the acquiring unit acquiring authentication data associated with the identity identifier from a blockchain network comprises:

if the verification result indicates that the digital signature is valid, acquiring the authentication data associated with the identity identifier from the blockchain network.

15. The authentication device according to claim 13 or 14, wherein the acquiring unit acquiring authentication data associated with the identity identifier from a blockchain network comprises:

sifting out the authentication data comprising the identity identifier from the blockchain network, and determining the obtained authentication data as the authentication data associated with the identity identifier.

16. The authentication device according to claim 15, wherein

the acquiring unit is configured to, if more than one piece of authentication data is

obtained after the sifting, determine authentication data satisfying a preset condition in the obtained authentication data, and determine the determined authentication data as the authentication data associated with the identity identifier.

17. The authentication device according to claim 16, wherein the preset condition comprises at least one or more of the following:

a generation time of the authentication data satisfies a preset time condition;

an institution identifier comprised in the authentication data satisfies a preset issuing institution's institution identifier; and

a service type comprised in the authentication data is the same as a service type of a service initiated by the user.

18. The authentication device according to claim 13 or 17, wherein the authentication unit performing identity authentication on the user according to the authentication data comprises:

determining a current authentication state of the identity identifier according to the authentication data; and

if the identity identifier is in an abnormal state and/or an authentication failed state, determining that the identity authentication on the user is not successful; otherwise, determining that the identity authentication on the user is successful.

19. The authentication device according to claim 18, wherein the authentication device further comprises a storage unit, wherein

the storage unit is configured to generate authentication data according to the authentication result, wherein the authentication data comprises the identity identifier of the user, an institution identifier of an institution that generates the authentication result, and the authentication result; and

store the authentication data to a blockchain node of the blockchain network.

20. The authentication device according to claim 19, wherein the authentication device further comprises a sending unit, wherein

the sending unit is configured to, before the authentication data is stored to a blockchain node of the blockchain network, send the authentication data to the blockchain network, so that the blockchain network performs consensus processing on the authentication data; and

the storage unit storing the authentication data to a blockchain node of the blockchain network comprises:

if the consensus processing result indicates that a consensus is reached, storing the authentication data to a blockchain node of the blockchain network.

21. The authentication device according to claim 18, wherein the authentication device further comprises a storage unit, wherein

the acquiring unit is configured to, after it is determined that the identity authentication on the user is successful, acquire, according to the service type of the service requested by the user, identity feature information of the user associated with the service type from an identity information management server; and

the storage unit is configured to generate authentication data according to the authentication result and the identity feature information, wherein the authentication data comprises the identity identifier of the user, an institution identifier of an institution that generates the authentication result, an authentication event of authenticating the identity feature information, and the authentication result; and

store the authentication data to a blockchain node of the blockchain network.

22. A blockchain-based authentication data processing device, comprising:

a receiving unit configured to receive identity information sent from a user, and authenticate the identity information;

a processing unit configured to generate first authentication data according to the authentication result, wherein the first authentication data comprises the authentication result, an institution identifier of an institution that generates the authentication result, and an identity identifier of the user, and wherein the authentication result comprises authentication being successful/authentication being failed; and

a storage unit configured to store the first authentication data to a blockchain node of a blockchain network.

23. The authentication data processing device according to claim 22, wherein the authentication data processing device further comprises an establishment unit, wherein

the establishment unit is configured to establish a mapping relationship between an identity identifier of the user and identity information of the user; and store the identity information of the user to an identity information database according to the mapping relationship.

24. The authentication data processing device according to claim 22, wherein the authentication data processing device further comprises a determining unit, wherein

the receiving unit is configured to receive a loss report or unregistration request sent from the user, wherein the loss report or unregistration request comprises the identity identifier of the user;

the determining unit is configured to determine according to the loss report or unregistration request that the identity information of the user is in an abnormal state;

the processing unit is configured to generate second authentication data according to the identity information of the user being in an abnormal state, the institution identifier of the institution that generates the authentication result, and the identity identifier of the user; and

the storage unit is configured to store the second authentication data to a blockchain

node of the blockchain network.

25. An authentication device, comprising at least one memory and at least one processor, wherein the at least one memory stores a program and the device is configured to execute the following steps by the at least one processor:

receiving an authentication request sent from a user, wherein the authentication request comprises an identity identifier of the user;

acquiring authentication data associated with the identity identifier from a blockchain network, wherein a blockchain node of the blockchain network stores a mapping relationship between identity identifiers and authentication data, the authentication data comprises an authentication result, and the authentication result comprises authentication being successful/authentication being failed; and

performing identity authentication on the user according to the authentication data.

26. A blockchain-based authentication data processing device, comprising at least one memory and at least one processor, wherein the at least one memory stores a program and the device is configured to execute the following steps by the at least one processor:

receiving identity information sent from a user, and authenticating the identity information;

generating first authentication data according to the authentication result, wherein the first authentication data comprises the authentication result, an institution identifier of an institution that generates the authentication result, and an identity identifier of the user, and wherein the authentication result comprises authentication being successful/authentication being failed; and

storing the first authentication data to a blockchain node of a blockchain network.