[0055] or, calling a verification function to verify the verification code, and returning indication information that the verification operation is running to the alliance chain.

[0056] In a third aspect, this application related to an apparatus for data acquisition, the apparatus including:

[0057] an acquisition module, configured for acquiring a data calling request sent by a first terminal, where, the data calling request carries a first decentralized identity of a data authorization user and an identity of a data calling user;

[0058] an authentication module, configured for performing identity authentication to the data calling user corresponding to the first terminal according to the data calling request;

[0059] an assignment module, configured for assigning a second decentralized identity to the data calling user when the data calling user is authenticated legal;

[0060] a querying module, configured for querying a data authorization certificate of the data authorization user by using the first decentralized identity according to the second decentralized identity;

[0061] a first sending module, configured for sending a data authorization request to a second terminal corresponding to the data authorization user according to the data authorization certificate; and

[0062] a second sending module, configured for encrypting the request result corresponding to the data calling request after confirming that the data authorization user confirms the authorization, and sending the encrypted request result to the first terminal.

[0063] In a fourth aspect, this application relates to an apparatus for data acquisition, the apparatus including:

[0064] a receiving module, configured for receiving a data authorization request sent by an alliance chain;

[0065] where, the data authorization request is sent by the alliance chain after: acquiring a data calling request sent by a first terminal; performing identity authentication to the data calling user corresponding to the first terminal according to the data calling request; assigning a second decentralized identity to the data calling user when the data calling user is authenticated legal; querying a data authorization certificate of the data authorization user by using the first decentralized identity according to the second decentralized identity; where, the data calling request carries a first decentralized identity of a data authorization user and an identity of a data calling user; and

[0066] an authorization module, configured for performing an authorization operation according to the data authorization request.

verification code to verify the verification code, and returns the indication information that the verification operation is running to the alliance chain.

[00133] In some embodiments, the verification code may be in a variety of forms such as pictures, letters or numbers.

[00134] The present application relates to a first apparatus for data acquisition 4, the implementation of which can be referred to in the description of the embodiment part of the method for data acquisition, and will not be illustrated repeatedly. As shown in Fig. 4:

[00135] an acquisition module 401, configured for acquiring a data calling request sent by a first terminal, where, the data calling request carries a first decentralized identity of a data authorization user and an identity of a data calling user;

[00136] an authentication module 402, configured for performing identity authentication to the data calling user corresponding to the first terminal according to the data calling request;

[00137] an assignment module 403, configured for assigning a second decentralized identity to the data calling user when the data calling user is authenticated legal;

[00138] a querying module 404, configured for querying a data authorization certificate of the data authorization user by using the first decentralized identity according to the second decentralized identity;

[00139] a first sending module 405, configured for sending a data authorization request to a second terminal corresponding to the data authorization user according to the data authorization certificate; and

[00140] a second sending module 406, configured for encrypting the request result corresponding to the data calling request after confirming that the data authorization user confirms the authorization, and sending the encrypted request result to the first terminal.

[00141] The present application relates to a second apparatus for data acquisition 5, the implementation of which can be referred to in the description of the embodiment part of the method for data acquisition, and will not be illustrated repeatedly. As shown in Fig.5:

[00142] a receiving module 501, configured for receiving a data authorization request sent by an alliance chain;

[00143] where, the data authorization request is sent by the alliance chain after: acquiring a data calling request sent by a first terminal; performing identity authentication to the data calling user corresponding to the first terminal according to the data calling request; assigning a second decentralized identity to the data calling user when the data calling user is authenticated legal; querying a data authorization certificate of the data authorization user by using the first decentralized identity according to the second decentralized identity; where, the data calling

CLAIMS

1. A method for data acquisition, applied to an alliance chain, the method for data acquisition comprising:

acquiring a data calling request sent by a first terminal, wherein, the data calling request carries a first decentralized identity of a data authorization user and an identity of a data calling user;

performing identity authentication to the data calling user corresponding to the first terminal according to the data calling request;

assigning a second decentralized identity to the data calling user when the data calling user is authenticated legal;

querying a data authorization certificate of the data authorization user by using the first decentralized identity according to the second decentralized identity;

sending a data authorization request to a second terminal corresponding to the data authorization user according to the data authorization certificate; and

encrypting the request result corresponding to the data calling request after confirming that the data authorization user confirms the authorization, and sending the encrypted request result to the first terminal.

2. The method for data acquisition according to claim 1, wherein, before querying the data authorization certificate of the data authorization user by using the first decentralized identity according to the second decentralized identity, the method further comprises:

acquiring a data preservation request sent by the second terminal, wherein, the data preservation request carries the identity of the data authorization user;

performing identity authentication to the data authorization user according to the data preservation request;

assigning the first decentralized identity to the data authorization user when the data authorization user is authenticated to be legal; and

distributing the data authorization certificate to the data authorization user according to the first decentralized identity.

3. The method for data acquisition according to claim 1 or 2, wherein the data calling request comprises: an identity type of the data calling user;

performing identity authentication to the data calling user corresponding to the first terminal according to the data calling request comprises:

performing identity authentication to the data calling user by using a face recognition technology when the identity type of the data calling user is individual; and

performing identity authentication to the data calling user by using an enterprise authentication technology when the identity type of the data calling user is enterprise.

4. The method for data acquisition according to claim 2 or 3, wherein, the data preservation request comprises: an identity type of the data authorization user;

performing identity authentication to the data authorization user according to the data preservation request, comprises:

performing identity authentication to the data authorization user by using the face recognition technology when the identity type of the data authorization user is the individual; and

performing identity authentication to the data authorization user by using the enterprise authentication technology when the identity type of the data authorization user is the enterprise.

5. The method for data acquisition according to any one of claims 1 to 4, wherein, sending the data authorization request to the second terminal corresponding to the data authorization user according to the data authorization certificate comprises:

initiating the data authorization request according to the data authorization certificate, and digitally signing the data authorization request by using a pre-stored private key, generating authorization request verification information, sending the authorization request verification information to the second terminal corresponding to the data authorization user.

6. The method for data acquisition according to claim 5, wherein the method further comprises:

acquiring indication information that a verification operation is running returned by the second terminal;

verifying the first decentralized identity of the data authorization user, and the data authorization certificate; and

sending indication information for executing a data authorization operation to the second terminal when the verification is legal.

7. The method for data acquisition according to claim 5 or 6, wherein the authorization request verification information comprises any one of a two-dimensional code, a bar code and a verification code;

generating the authorization request verification information, sending the authorization request verification information to the second terminal corresponding to the data authorization user comprises:

generating the two-dimensional code and sending the two-dimensional code to the second terminal corresponding to the data authorization user;

or, generating the bar code and sending the bar code to the second terminal corresponding to the data authorization user;

or, generating the verification code and sending the verification code to the second terminal corresponding to the data authorization user.

8. The method for data acquisition according to any one of claims 1 to 7, wherein the data calling request further comprises: a data authorization certificate type; and

querying the data authorization certificate of the data authorization user by using the first decentralized identity according to the second decentralized identity comprises:

querying the data authorization certificate type corresponding to the data authorization certificate type in the data calling request, by using the first decentralized identity according to the second decentralized identity.

9. The method for data acquisition according to any one of claims 1 to 8, further comprising:

calculating hash values of an identity authentication record corresponding to the identity authentication, the data authorization certificate, the data authorization request and a data authorization record corresponding to the data authorization request respectively by using a hash algorithm, and storing the hash values in the alliance chain.

10. A method for data acquisition, applied to a second terminal, the method for data acquisition comprising:

receiving a data authorization request sent by an alliance chain;

wherein, the data authorization request is sent by the alliance chain after: acquiring a data calling request sent by a first terminal; performing identity authentication to the data calling user corresponding to the first terminal according to the data calling request; assigning a second decentralized identity to the data calling user when the data calling user is authenticated legal; querying a data authorization certificate of the data authorization user by using the first decentralized identity according to the second decentralized identity; wherein, the data calling request carries a first decentralized identity of a data authorization user and an identity of a data calling user; and

performing an authorization operation according to the data authorization request.

11. The method for data acquisition according to claim 10, wherein receiving the data authorization request sent by the alliance chain comprises:

receiving authorization request verification information sent by the alliance chain;

performing the authorization operation according to the data authorization request comprises:

verifying the authorization request verification information, and returning indication information that the verification operation is running to the alliance chain;

receiving indication information for executing a data authorization operation sent by the alliance chain; and

executing an authorization operation according to the indication information for executing the data authorization operation, and digitally signing the authorization operation by using a pre-stored private key.

12. The method for data acquisition according to claim 11, wherein the authorization request verification information comprises any one of a two-dimensional code, a bar code and a verification code;

verifying the authorization request verification information, and returning indication information that the verification operation is running to the alliance chain comprises:

calling a code scanning function to scan the two-dimensional code, and returning indication information that the verification operation is running to the alliance chain;

or, calling a code scanning function to scan the bar code, and returning indication information that the verification operation is running to the alliance chain;

or, calling a verification function to verify the verification code, and returning indication information that the verification operation is running to the alliance chain.

13. A first apparatus for data acquisition, comprising:

an acquisition module, configured for acquiring a data calling request sent by a first terminal, wherein, the data calling request carries a first decentralized identity of a data authorization user and an identity of a data calling user;

an authentication module, configured for performing identity authentication to the data calling user corresponding to the first terminal according to the data calling request;

an assignment module, configured for assigning a second decentralized identity to the data calling user when the data calling user is authenticated legal;

a querying module, configured for querying a data authorization certificate of the data authorization user by using the first decentralized identity according to the second decentralized identity;

a first sending module, configured for sending a data authorization request to a second terminal corresponding to the data authorization user according to the data authorization certificate; and

a second sending module, configured for encrypting the request result corresponding to the data calling request after confirming that the data authorization user confirms the authorization, and sending the encrypted request result to the first terminal.

14. A second apparatus for data acquisition, comprising:

a receiving module, configured for receiving a data authorization request sent by an alliance chain;

wherein, the data authorization request is sent by the alliance chain after: acquiring a data calling request sent by a first terminal; performing identity authentication to the data calling user corresponding to the first terminal according to the data calling request; assigning a second decentralized identity to the data calling user when the data calling user is authenticated legal; querying a data authorization certificate of the data authorization user by using the first decentralized identity according to the second decentralized identity; wherein, the data calling request carries a first decentralized identity of a data authorization user and an identity of a data calling user; and

an authorization module, configured for performing an authorization operation according to the data authorization request.

15. An electronic device comprises a processor, a communication component, a memory and a communication bus, wherein the processor, the communication component and the memory communicate with each other through the communication bus;

the memory is configured for storing computer programs; and

the processor is configured to implement the method for data acquisition applied to an alliance chain according to any one of claims 1 to 9, or to implement the method for data acquisition applied to a second terminal according to any one of claims 10 to 12.

16. A computer-readable storage medium, wherein a program is stored on the computer-readable storage medium, wherein, the program, when executed by a processor, implements the method for data acquisition applied to an alliance chain according to any one of claims 1 to 9, or implements the method for data acquisition applied to a second terminal according to any one of claims 10 to 12.