

What Is Claimed Is

1. A computer-executed method, comprising:
 - receiving, by a digital identity client executing on a computer, an identity-verification request comprising an identifier of a user;
 - sending, by the digital identity client to an identity-verification-service-publishing blockchain network, a query for available identity-verification services;
 - determining an identity-verification server based on a result of the query;
 - verifying identity of the user based on the identity-verification server;
 - generating a public-private key pair comprising a public key and a private key corresponding to the identifier of the user;
 - storing, in an identity-verification blockchain network, identity-verification information corresponding to the user, wherein the identity-verification information is associated with the public-private key pair for the user, thereby facilitating subsequent identity verification of the user;
 - receiving, by the digital identity client from an application requiring identity verification of the user, a first request comprising the identifier of the user and first information; and
 - transmitting the public key corresponding to the identifier of the user and signed data to the application, wherein the signed data is generated by signing the first information using the corresponding private key, thereby facilitating the application in performing identity verification of the user,
 - wherein the identity-verification blockchain network comprises nodes located in different countries or regions, and wherein a first node of the identity-verification blockchain network and the application belong to a same country or region.

2. The method according to claim 1, further comprising:
sending, by the application, a checking request to a first node of the identity-verification blockchain network, wherein the checking request comprises the signed data and the public key, thereby facilitating the first node to perform checking based on the signed data and the public key;
receiving, by the application, a checking result from the first node of the identity-verification blockchain network; and
performing identity verification of the user according to the checking result.

3. The method according to claim 2:
wherein the identity-verification information stored in the identity-verification blockchain network further comprises: a hash value of the public key, a type of identity verification that successfully validates the user's identity, and a hash value of the identifier of the user;
wherein the checking request further comprises a hash value of the identifier of the user; and
wherein the first node performs the checking by:
computing a hash value of the public key included in the checking request;
searching the identity-verification blockchain network for an identifier hash value and a type of identity verification that successfully validates the user's identity corresponding to the computed hash value of the public key;
performing signature validation on the signed data in the checking request using the public key; and
in response to the searched identifier hash value matching the identifier of the user in the checking request and the signature validation

being successful, sending to the application the searched type of identity verification that successfully validates the user's identity as the checking result.

4. The method according to claim 3, further comprising:

in response to determining, by the application, that the type of identity verification that successfully validates the user's identity in the checking result does not meet a service requirement, querying a second node of the identity-verification-service-publishing blockchain network for an identity verification service meeting the service requirement;

sending a second identification-verification request, by the application to the digital identity client, which forwards the second identification-verification request to a server associated with the identity verification service meeting the service requirement, wherein the second identification-verification request comprises the signed data and the public key; and

performing, by the server associated with the identity verification service meeting the service requirement, identity validation of the user and updating the identity-verification information stored in the identity-verification blockchain network.

5. The method according to claim 4, wherein the identity-verification-service-publishing blockchain network comprises nodes located in different countries or regions, and wherein the second node of the identity-verification-service-publishing blockchain network and an object requiring identity verification belong to the same country or region.

6. The method according to claim 3, wherein updating the identity-verification information stored in the identity-verification blockchain network further comprises:

sending, by the server associated with the identity verification service meeting the service requirement, to a third node of the identity-verification blockchain network the signed data and the public key;

performing, by the third node, signature checking on the signed data based on the public key; and

in response to the signature checking being successful, updating the identity-verification information corresponding to the public key.

7. The method according to claim 1, wherein the first information comprises one or more of: a service identifier and a random number.

8. The method according to claim 1, wherein the determined identity-verification server is located in a domiciled country or region associated with the user.

9. The method according to claim 1, further comprising:
sending, by an identity-verification server, to a fourth node of the identity-verification-service-publishing blockchain network information associated with the available identity-verification services, wherein the fourth node and the identity-verification server belong to the same country or region; and

storing, by the fourth node, the information associated with the available identity-verification services in the identity-verification-service-publishing blockchain network, and publishing the information to other nodes of the identity-verification-service-publishing blockchain network.

10. A computer system, comprising:

a processor;

a storage device coupled to the processor and storing instructions, which

when executed by the processor cause the processor to perform a method, the method comprising:

- receiving, by a digital identity client, an identity-verification request comprising an identifier of a user;

- sending, by the digital identity client to an identity-verification-service-publishing blockchain network, a query for available identity-verification services;

- determining an identity-verification server based on a result of the query;

- verifying identity of the user based on the identity-verification server;

- generating a public-private key pair comprising a public key and a private key corresponding to the identifier of the user;

- storing, in an identity-verification blockchain network, identity-verification information corresponding to the user, wherein the identity-verification information is associated with the public-private key pair, thereby facilitating subsequent identity verification of the user;

- receiving, by the digital identity client from an application requiring identity verification of the user, a first request comprising the identifier of the user and first information; and

- transmitting the public key corresponding to the identifier of the user and signed data to the application, wherein the signed data is generated by signing the first information using the corresponding private key, thereby facilitating the application in performing identity verification of the user,

- wherein the identity-verification blockchain network comprises nodes located in different countries or regions, and wherein a first node of the identity-verification blockchain network and the application belong to a same country or region.

11. The computer system according to claim 10, wherein the method further comprises:

sending, by the application, a checking request to a first node of the identity-verification blockchain network, wherein the checking request comprises the signed data and the public key, thereby facilitating the first node to perform checking based on the signed data and the public key;

receiving, by the application, a checking result from the first node of the identity-verification blockchain network; and

performing identity verification of the user according to the checking result.

12. The computer system according to claim 11:

wherein the identity-verification information stored in the identity-verification blockchain network further comprises: a hash value of the public key, a type of identity verification that successfully validates the user's identity, and a hash value of the identifier of the user;

wherein the checking request further comprises a hash value of the identifier of the user; and

wherein the first node performs the checking by:

computing a hash value of the public key included in the checking request;

searching the identity-verification blockchain network for an identifier hash value and a type of identity verification that successfully validates the user's identity corresponding to the computed hash value of the public key;

performing signature validation on the signed data in the checking request using the public key; and

in response to the searched identifier hash value matching the identifier of the user in the checking request and the signature validation being successful, sending to the application the searched type of

identity verification that successfully validates the user's identity as the checking result.

13. The computer system according to claim 12, wherein the method further comprises:

in response to determining, by the application, that the type of identity verification that successfully validates the user's identity in the checking result does not meet a service requirement, querying a second node of the identity-verification-service-publishing blockchain network for an identity verification service meeting the service requirement;

sending a second identification-verification request, by the application to the digital identity client, which forwards the second identification-verification request to a server associated with the identity verification service meeting the service requirement, wherein the second identification-verification request comprises the signed data and the public key; and

performing, by the server associated with the identity verification service meeting the service requirement, identity validation of the user and updating the identity-verification information stored in the identity-verification blockchain network.

14. The computer system according to claim 13, wherein the identity-verification-service-publishing blockchain network comprises nodes located in different countries or regions, and wherein the second node of the identity-verification-service-publishing blockchain network and an object requiring identity verification belong to the same country or region.

15. The computer system according to claim 12, wherein updating the identity-verification information stored in the identity-verification blockchain network further comprises:

sending, by the server associated with the identity verification service meeting the service requirement, to a third node of the identity-verification blockchain network the signed data and the public key;

performing, by the third node, signature checking on the signed data based on the public key; and

in response to the signature checking being successful, updating the identity-verification information corresponding to the public key.

16. The computer system according to claim 10, wherein the first information comprises one or more of: a service identifier and a random number.

17. The computer system according to claim 10, wherein the determined identity-verification server is located in a domiciled country or region associated with the user.

18. The computer system according to claim 10, wherein the method further comprises:

sending, by an identity-verification server, to a fourth node of the identity-verification-service-publishing blockchain network information associated with the available identity-verification services, wherein the fourth node and the identity-verification server belong to the same country or region; and

storing, by the fourth node, the information about the available identity-verification services in the identity-verification-service-publishing blockchain network, and publishing the information to other nodes of the identity-verification-service-publishing blockchain network.