

CLAIMS

What is claimed is:

1. A cross-blockchain authentication method for cross-blockchain authentication, the method comprising:

obtaining, by a subscribing client included in a system for cross-chain interaction, a public key of an oracle engine connected to a second blockchain, the system comprising the subscribing client, a publishing client, and a cross-chain interaction end, wherein the subscribing client corresponds to a first blockchain, the publishing client corresponds to the second blockchain, the cross-chain interaction end being separately connected to the subscribing client and the publishing client (402);

using the public key as an authentication data source (402);

obtaining, by using the cross-chain interaction end, data that is to be authenticated in the second blockchain and is published by the publishing client, wherein the data to be authenticated is signed by the oracle engine based on a private key held by the oracle engine (404); and

performing, based on the authentication data source and a signature of the data to be authenticated, data authentication on the data to be authenticated (406).

2. The method according to claim 1, wherein obtaining the public key comprises:

obtaining the public key that is configured by a user and is of the oracle engine corresponding to the second blockchain, and using the public key as the authentication data source.

3. The method according to claim 1, wherein obtaining the public key comprises:

obtaining, by using the cross-chain interaction end, the public key that is published by the publishing client and is of the oracle engine corresponding to the second blockchain, and using the public key as the authentication data source.

4. The method according to any one of claims 1 to 3, wherein obtaining the data that is to be authenticated comprises:

initiating a subscription request to the cross-chain interaction end, wherein the

subscription request is used to indicate subscription conditions to the cross-chain interaction end, so that the cross-chain interaction end requests, from the publishing client based on the subscription conditions, data that is to be authenticated in the second blockchain and satisfies the subscription conditions; and

obtaining data that is to be authenticated and is published by the publishing client, wherein the data to be authenticated satisfies the subscription conditions, and is signed by the oracle engine based on the private key held by the oracle engine.

5. The method according to any one of claims 1 to 4, wherein performing the data authentication comprises:

verifying, based on the stored public key of the oracle engine in the authentication data source, the signature of the data to be authenticated; and if the verification on the signature succeeds, determining that the data authentication on the data to be authenticated succeeds.

6. The method according to any one of claims 1 to 5, wherein the publishing client is connected to the oracle engine, and the oracle engine is configured to perform operations comprising:

performing data authentication on data in the second blockchain;
after the data authentication succeeds, signing, based on the private key held by the oracle engine, data that is successfully authenticated; and
actively pushing the signed data to the publishing client; or
pushing the signed data to the publishing client in response to a data acquisition request of the publishing client.

7. The method according to any one of claims 1 to 6, wherein the oracle engine corresponding to the second blockchain is the publishing client.

8. The method according to any one of claims 1 to 7, wherein the subscribing client corresponds to a node device in the first blockchain, and the publishing client and the oracle engine correspond to a node device in the second blockchain.

9. The method according to any one of claims 1 to 8, wherein the data comprises one of a transaction, a block, a state, and an event.
10. The method according to any one of claims 1 to 9, wherein the authentication data source depends on a data authentication protocol supported by the first blockchain and the second blockchain.
11. The method according to any one of claims 1 to 10, wherein the authentication rule comprises an authentication logic that depends on a specific type of the data recorded on the second blockchain.
12. An apparatus for cross-blockchain authentication, the apparatus comprising a plurality of modules configured to perform the method of any one of claims 1 to 11.