

CLAIMS

What is claimed is:

1. A method for cross-blockchain authentication, the method comprising:
obtaining, by a subscribing client by using a cross-chain client of a cross-blockchain interaction system, data from a second blockchain that is published by a publishing client, to use the data as an authentication data source, the cross-blockchain interaction system comprising the subscribing client, the publishing client, and a cross-chain client, the subscribing client corresponds to a first blockchain, the publishing client corresponds to the second blockchain, the cross-chain client is separately interconnected with the subscribing client and the publishing client and the first blockchain being used as a sidechain that is anchored to the second blockchain that is used as a main chain (302);
receiving data to be authenticated from the second blockchain (304); and
performing data authentication on the data to be authenticated based on the authentication data source and a data authentication rule configured on the first blockchain (306).
2. The method according to claim 1, wherein obtaining the data comprises:
initiating, by the subscribing client, a subscription request to a cross-chain interaction end, wherein the subscription request is used to notify the cross-chain interaction end of a subscription condition, so that the cross-chain interaction end requests, based on the subscription condition, data on the second blockchain that satisfies the subscription condition from the publishing client; and
obtaining, by the subscribing client, the data on the second blockchain that is published by the publishing client and that satisfies the subscription condition, to use the data as the authentication data source.
3. The method according to claim 2, wherein the authentication data source comprises block header data of each block on the second blockchain.

4. The method according to claim 3, wherein performing data authentication on the data to be authenticated based on the authentication data source and the data authentication rule configured on the first blockchain comprises:

performing simplified payment verification (SPV) data authentication on the data to be authenticated based on the authentication data source and the data authentication rule configured on the first blockchain, to determine whether the data to be authenticated is comprised in the block on the second blockchain.

5. The method according to claim 4, wherein performing SPV data authentication on the data to be authenticated based on the authentication data source and the data authentication rule configured on the first blockchain comprises:

calculating a hash value of the data to be authenticated (402);

obtaining a Merkle authentication path of the data to be authenticated on a Merkle tree of a target block on the second blockchain that comprises the data to be authenticated (404);

calculating a hash value of a block header of the target block based on the hash value of the data to be authenticated and a hash value of each node on the Merkle authentication path (406);

determining whether the calculated hash value of the block header of the target block matches a hash value that is of the block header of the target block and that is stored in the authentication data source (408); and

if yes, determining that the data to be authenticated is comprised in the block on the second blockchain (408).

6. The method according to any one of claims 1 to 5, wherein the subscribing client corresponds to a node device on the first blockchain, and the publishing client corresponds to a node device on the second blockchain.

7. The method according to any one of claims 1 to 6, wherein the data comprises one of a transaction, a status, and an event.

8. The method according to any one of claims 1 to 7, wherein the authentication data source depends on a data authentication protocol supported by the first blockchain and the second blockchain.
9. The method according to any one of claims 1 to 8, wherein the authentication rule comprises an authentication logic that depends on a specific type of the data recorded on the second blockchain.
10. 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 9.