

CLAIMS

What is claimed is:

1. A computer-implemented method performed by a blockchain-based data verification system, wherein the blockchain-based data verification system comprises a first verification system, a second verification system, a first blockchain node and a second blockchain node on a blockchain network, the method comprising:

collecting, by the first verification system, first service data based on a predetermined condition, wherein the first service data comprises pieces of transaction service data of a first service system and the predetermined condition is the obtaining, by the first verification system and from the first service system, of a number of pieces of transaction service data of the first service system that reaches a predetermined threshold N, wherein N is a positive integer;

generating, by the first verification system, a first verification file including the first service data;

processing, by the first verification system, the first verification file to generate a first digital digest;

sending, by the first verification system, a verification request to the second verification system, the verification request including the first verification file and the first digital digest;

receiving, by the second verification system, second service data from a second service system, wherein the second service data is transaction service data of the second service system, and storing the second service data in a local database of the second verification system;

receiving, by the second verification system, the verification request from the first verification system;

extracting, by the second verification system, the first digital digest from the verification request;

validating, by the second verification system, the first service data in the first verification file based on the first digital digest;

in response to that the validating the first service data succeeds, determining, by the second verification system, the second service data corresponding to the first service data based on identification information in the first service data;

obtaining, by the second verification system, a verification rule for the second service data, the verification rule corresponding to critical service information in the second service data;

5 verifying, by the second verification system, the first service data with the second service data based on the verification rule;

generating, by the second verification system, a verification result notification;

sending, by the second verification system, the verification result notification to the first verification system;

receiving, by the first verification system, the verification result notification;

10 sending, by the first verification system, successfully verified first service data to the second blockchain node on the blockchain network;

sending, by the second verification system, successfully verified second service data in the local database to the first blockchain node on the blockchain network;

15 after receiving and storing, by the second blockchain node, the successfully verified first service data that is sent by the first verification system and receiving and storing, by the first blockchain node, the successfully verified second service data that is sent by the second verification system, transmitting, by the second blockchain node and the first blockchain node, the successfully verified first service data and the successfully verified second service data to other blockchain nodes for the blockchain nodes of the blockchain network to reach a consensus on the successfully verified first service data and the successfully verified second service data and store the successfully verified first service data and the successfully verified second service data in a blockchain of the blockchain network.

2. The method according to claim 1, wherein the first service data includes, for a piece of data of the first service data, identification information of the piece of data, critical service information of the piece of data, and a verification status of the piece of data; and

25 wherein the second service data includes, for a piece of data of the second service data, identification information of the piece of data, critical service information of the piece of data, and a verification status of the piece of data.

3. The method according to claim 2, wherein the first service data is sent by the first service system to the first verification system and the second service data is sent by the second service system to the second verification system.

4. The method according to claim 1, comprising the following steps performed by
5 the first verification system:

obtaining pieces of transaction service data of the first service system; and

storing the obtained pieces of transaction service data of the first service system as the first verification file in response to that the number of the obtained pieces of transaction service data of the first service system reaches the predetermined threshold

10 N.

5. The method according to claim 1, further comprising the following steps performed by the second verification system:

generating a second verification file based on a result of the verifying the first service data with the second service data;

15 processing the second verification file to generate a second digital digest; and

sending the verification result notification to the first verification system, the verification result notification including the second verification file and the second digital digest corresponding to the second verification file.

6. A blockchain-based data verification system comprising a first verification
20 system, a second verification system, a first blockchain node and a second blockchain node on a blockchain network, wherein the blockchain-based data verification system is configured to carry out the steps of the method according to any one of claims 1 to 5.