

CLAIMS

What is claimed is:

1. A computer-implemented method performed by a blockchain-based data verification system, ~~comprising: wherein the blockchain-based data verification system~~
5 comprises a first verification system, a second verification system, ~~and~~ a first blockchain node and a second blockchain node on a blockchain network; the method comprising:
collecting, by the first verification system~~configured to: collect,~~ first service data based on a predetermined condition, wherein the first service data comprises pieces of
10 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;
and~~generate~~generating, by the first verification system, a first verification file
15 including the first service data; ~~;~~
processing, by the first verification system, the first verification file to generate a first digital digest;
and~~sends~~sending, by the first verification system, a verification request to the second verification system, the verification request including the first verification file
20 and the first digital digest;
receiving, by the second verification system~~configured to: receive the verification request, verify the first service data in the first verification file with,~~ 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
25 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;
30 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
5 service data, the verification rule corresponding to critical service information in the
second service data;
verifying, by the second verification system, the first service data with the second
service data based on the verification rule;
and generategenerating, by the second verification system, a verification result
10 notification;
send 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;
sending, by the first verification system, successfully verified first service data to
15 the second blockchain node on the blockchain network;
and send sending, by the second verification system, successfully verified second
service data in the local database to the first blockchain node on the blockchain network;
~~the first verification system further configured to: receive the verification result~~
~~notification, and send successfully verified first service data to the second blockchain~~
20 ~~node on the blockchain network;~~
~~the first blockchain node configured to receive and store the successfully verified~~
~~second service data that is sent by the second verification system; and~~
~~the second blockchain node configured to receive and store the successfully~~
~~verified first service data that is sent by the first verification system.~~
25 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
30 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 system-method according to claim 1, ~~further comprising: a first service system and a second service system; wherein~~

5 ~~the first service system configured to send the first service data to the first verification system, the first service data including~~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

10 ~~the second service system configured to send the second service data to the second verification system; wherein~~ the second service data ~~including~~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; ~~and~~

15 ~~the second verification system further configured to receive the second service data of the second service system and store the second service data in the local database~~

3. The system-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; ~~is further configured to: determine a verification rule corresponding to the second service data based on the second service data, determine a mapping relationship between the second service data and the verification rule, and store the mapping relationship between the second service data and the verification rule in the local database.~~

20

25 4. The method according to claim 1, comprising the following steps performed by 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
30 transaction service data of the first service system reaches the predetermined threshold N.~~The system according to claim 1, wherein the first verification system is further configured to: obtain the first service data, store N pieces of the first service data as the first verification file in response to that a number of pieces of the first service data~~

reaches a predetermined threshold N and process the first verification file to generate a first digital digest, and send the verification request to the second verification system, the verification request including the first verification file and the first digital digest corresponding to the first verification file.

5

~~5. The system according to claim 1, wherein the second verification system is further configured to: receive the verification request, extract a first digital digest from the verification request, and validate the first service data in the first verification file based on the first digital digest; and~~

10

~~in response to that the validating the first service data succeeds, determine the second service data corresponding to the first service data based on identification information in the first service data, obtain a verification rule for the second service data, verify the first service data with the second service data based on the verification rule and generate the verification result notification, and send the verification result notification to the first verification system.~~

15

~~5.6. The system according to claim 5, wherein the second verification system is further configured to: verify the first service data with the second service data based on the verification rule; The method according to claim 1, further comprising the following steps performed by the second verification system:~~

20

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

~~process~~ing the second verification file to generate a second digital digest; ~~and~~

25

~~sending~~ing 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 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.

30

~~7. The system according to claim 1, wherein the first verification system is further configured to: extract a second verification file and a second digital digest that are~~

~~included in the verification result notification, validate the second verification file based on the second digital digest, and in response to that the validating the second verification file succeeds, extract and upload the successfully verified first service data in the second verification file to the blockchain network.~~

5

~~8. The system according to claim 7, wherein the first verification system is further configured to: if unsuccessfully verified first service data exists in the second verification file, update a verification status of the unsuccessfully verified first service data and review or report the unsuccessfully verified first service data.~~

10

~~9. A blockchain-based data verification method, comprising, at a first verification system:~~

~~collecting first service data based on a predetermined condition and generating a first verification file including the first service data, the first service data including, for a piece of 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;~~

15

~~sending a verification request to a second verification system, the verification request including the first verification file; and~~

~~receiving a verification result notification sent by the second verification system, and sending successfully verified first service data to a second blockchain node.~~

20

~~10. The method according to claim 9, wherein collecting the first service data based on the predetermined condition and generating the first verification file including the first service data includes:~~

25

~~obtaining first service data of a first service system;~~

~~storing N pieces of the first service data as the first verification file in response to that a number of pieces of the first service data reaches a predetermined threshold N and processing the first verification file to generate a first digital digest; and~~

~~sending the verification request to the second verification system, the verification request including the first verification file and the first digital digest corresponding to the first verification file.~~

30

~~11. The method according to claim 9, wherein the verification result notification includes a second verification file and a second digital digest corresponding to the second verification file;~~

~~receiving the verification result notification sent by the second verification system;~~
5 ~~and sending the successfully verified first service data to the second blockchain node includes:~~

~~extracting the second verification file and the second digital digest that are included in the verification result notification, and validating the second verification file based on the second digital digest;~~

10 ~~in response to that the validating the second verification file succeeds, extracting and uploading the successfully verified first service data in the second verification file to the second blockchain node on a blockchain network; and~~

~~if unsuccessfully verified first service data exists in the second verification file, updating a verification status of the unsuccessfully verified first service data and~~
15 ~~reviewing or reporting the unsuccessfully verified first service data.~~

~~12. A blockchain-based data verification method, comprising, at a second verification system:~~

~~obtaining second service data of a second service system and storing the second~~
20 ~~service data in a local database;~~

~~receiving a verification request, the verification request including a first verification file;~~

~~verifying first service data in the first verification file with the second service data in the local database and generating a verification result notification, and sending the~~
25 ~~verification result notification to a first verification system; and~~

~~sending successfully verified second service data in the local database to a first blockchain node on a blockchain network.~~

~~13. The method according to claim 12, further comprising: before receiving the~~
30 ~~verification request,~~

~~determining a verification rule corresponding to the second service data based on the second service data;~~

determining a mapping relationship between the second service data and the verification rule; and

storing the mapping relationship between the second service data and the verification rule in the local database.

5

14. The method according to claim 12, further comprising: after receiving the verification request of a first service system;

extracting a first digital digest from the verification request and validating the first service data in the first verification file based on the first digital digest; and

10 in response to that the validating the first service data succeeds, verifying the first service data in the first verification file with the second service data in the local database.

15. The method according to claim 12, wherein verifying the first service data in the first verification file with the second service data in the local database and generating the verification result notification includes:

15

determining the second service data corresponding to the first service data based on identification information in the first service data;

obtaining a verification rule corresponding to critical service information in the second service data; and

20

verifying the first service data with the second service data in the local database based on the verification rule and generating the verification result notification based on a verification result.

16. The method according to claim 15, wherein generating the verification result notification based on the verification result includes:

25

generating a second verification file based on the verification result;

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

generating the verification result notification based on the second verification file and the second digital digest.

30

17. The method according to claim 16, wherein generating the second verification file based on the verification result includes:

In response to all of the first service data in the first verification file is successfully verified, updating a verification status in the first verification file and then generating the second verification file; and

5 In response to unsuccessfully verified first service data exists in the second verification file, the generated second verification file includes identification information, a verification status, and a verification failure cause that are of each piece of the first service data in the first verification file.

10 18. A computing device, comprising a memory, a processor, and a computer instruction stored in the memory and executable on the processor, wherein the steps of the method according to any one of claims 9 to 17 are implemented when the processor executes the instruction.

15 19. A computer readable storage medium, wherein the computer readable storage medium stores a computer instruction, and the steps of the method according to any one of claims 9 to 17 are implemented when the instruction is executed by a processor.