

CLAIMS

1. A blockchain-based data verification method, comprising:

obtaining (102) a data identifier of target data published by a data provider in
5 a blockchain, wherein the data identifier indicates a storage location of the target data in the blockchain;

determining (104) whether the target data has been stored in the blockchain based on the data identifier;

in response to determining that no target data corresponding to the data
10 identifier is stored in the blockchain, indicating that the data identifier published by the data provider is a false data identifier;

in response to determining that the target data has been stored in the blockchain, obtaining (106) the target data from the storage location indicated by the data identifier, wherein the target data stored in the blockchain comprises
15 verification information used to verify authenticity of the target data and auxiliary information related to authenticity verification, wherein the verification information is a first hash value obtained by performing a hash calculation based on original content of the target data and the auxiliary information, wherein the auxiliary information comprises an identifier of a data uploader, an upload
20 timestamp of the target data, and an upload location of the target data, wherein the upload location includes an address description;

executing an installed verification program to verify authenticity of the obtained target data based on the verification information;

performing a hash calculation on the original content of the target data and the
25 auxiliary information to obtain a second hash value;

determining whether the second hash value is the same as the first hash value carried in the target data stored in the blockchain;

if yes, determining that the obtained target data passed the authenticity verification, or if not, determining that the obtained target data has failed to pass the
30 authenticity verification; and

outputting a verification result to a data verifier.

2. The method according to claim 1, wherein the target data published by the data provider carries a graphic code generated based on the data identifier;

35 and

obtaining (102) a data identifier of target data published by a data provider in a blockchain comprises:

scanning and parsing the graphic code to obtain the data identifier of the target data in the blockchain.

5

3. The method according to claim 1 or 2, wherein the data identifier is a transaction hash value of a transaction of the target data; and
determining (104) whether the target data has been stored in the blockchain based on the data identifier comprises:

10 performing Simplified Payment Verification, SPV, for the transaction based on a transaction hash value of the transaction of the target data, to determine whether the transaction has been stored in the blockchain.

4. The method according to claim 1, further comprising:

15 outputting the target data obtained from the storage location indicated by the data identifier to the data verifier, so that the data verifier compares the outputted target data with the target data published by the data provider.

5. A blockchain-based data verification apparatus (40), comprising:

20 a first acquisition module (401), configured to obtain (102) a data identifier of target data published by a data provider in a blockchain, wherein the data identifier indicates a storage location of the target data in the blockchain;

a determining module (402), configured to determine (104) whether the target data has been stored in the blockchain based on the data identifier, and if it is
25 determined that no target data corresponding to the data identifier is stored in the blockchain, indicate that the data identifier published by the data provider is a false data identifier;

a second acquisition module (403), configured to: if the target data has been stored in the blockchain, obtain (106) the target data from the storage location indicated
30 by the data identifier, wherein the target data stored in the blockchain comprises verification information used to verify authenticity of the target data and auxiliary information related to authenticity verification,

wherein the verification information is a first hash value obtained by performing a hash calculation based on original content of the target data and the auxiliary
35 information, wherein the auxiliary information comprises an identifier of a data

uploader, an upload timestamp of the target data, and an upload location of the target data, wherein the upload location includes an address description; and a verification module (404), configured to:

- execute an installed verification program to verify authenticity of the obtained target data based on the verification information,
perform a hash calculation on the original content of the target data and the auxiliary information to obtain a second hash value,
determine whether the second hash value is the same as the first hash value carried in the target data stored in the blockchain,
if yes, determine that the obtained target data passed the authenticity verification, or if not, determine that the obtained target data has failed to pass the authenticity verification, and
output a verification result to a data verifier.

6. The apparatus (40) according to claim 5, wherein the target data published by the data provider carries a graphic code generated based on the data identifier; and
the first acquisition module (401) is configured to:
scan and parse the graphic code to obtain the data identifier of the target data in the blockchain.

7. The apparatus (40) according to claim 5 or 6, the data identifier is a transaction hash value of a transaction of the target data; and
the determining module (402) is configured to:
perform Simplified Payment Verification, SPV, for the transaction based on a transaction hash value of the transaction of the target data, to determine whether the transaction has been stored in the blockchain.

8. The apparatus (40) according to claim 5, wherein the second acquisition module (403) is further configured to:
output the target data obtained from the storage location indicated by the data identifier to the data verifier, so that the data verifier compares the outputted target data with the target data published by the data provider.