

CLAIMS

What is claimed is:

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

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

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

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

if the target data has been stored in the blockchain, obtaining the target data from the storage location indicated by the data identifier, wherein the target data stored in the blockchain carries verification information used to verify authenticity of the target
15 data, wherein the verification information is a hash value obtained by performing a hash calculation based on original content of the target data and auxiliary information;

verifying authenticity of the obtained target data based on the verification information; and

outputting a verification result to a data verifier.

20 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; and

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

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

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 whether the target data has been stored in the blockchain based on the data identifier comprises:

30 performing 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, wherein verifying authenticity of the obtained target data based on the verification information comprises:

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

5 invoking a smart contract published in the blockchain, executing a verification program defined in the smart contract, and verifying authenticity of the obtained target data based on the verification information.

5. The method according to claim 4, wherein the target data stored in the blockchain further comprises the auxiliary information related to the authenticity verification; and

10 verifying authenticity of the obtained target data based on the verification information comprises:

performing the hash calculation on the original content of the target data and the auxiliary information to obtain the hash value; determining whether the calculated
15 hash value is the same as a hash value carried in the target data stored in the blockchain; and 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 authenticity verification.

6. The method according to claim 5, wherein the auxiliary information comprises
20 any one of or a combination of at least two of the following:

an identifier of a data uploader;

an upload timestamp of the target data; or

an upload location of the target data.

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

25 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.

8. A blockchain-based data verification apparatus, comprising:

a first acquisition module, configured to obtain a data identifier of target data
30 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, configured to determine whether the target data has been stored in the blockchain based on the data identifier;

an indicating module, configured to: if it is 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, configured to: if the target data has been stored in the blockchain, obtain the target data from the storage location indicated by the data identifier, wherein the target data stored in the blockchain carries verification information used to verify authenticity of the target data, wherein the verification information is a hash value obtained by performing a hash calculation based on original content of the target data and auxiliary information;

a verification module, configured to: verify authenticity of the obtained target data based on the verification information; and

an output module, configured to output a verification result to a data verifier.

9. The apparatus according to claim 8, wherein the target data published by the data provider carries a graphic code generated based on the data identifier; and

the first acquisition module is configured to:

scan and parse the graphic code to obtain the data identifier of the target data in the blockchain.

10. The apparatus according to claim 8 or 9, wherein the data identifier is a transaction hash value of a transaction of the target data; and

the determining module is configured to:

perform 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.

11. The apparatus according to claim 8, wherein the verification module is further configured to:

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

invoke a smart contract published in the blockchain, execute a verification program defined in the smart contract, and verify authenticity of the obtained target data based on the verification information.

12. The apparatus according to claim 11, wherein the target data stored in the blockchain further comprises the auxiliary information related to the authenticity verification; and

the verification module is further configured to:

perform the hash calculation on the original content of the target data and the

auxiliary information to obtain the hash value; determine whether the calculated hash value is the same as a hash value carried in the target data stored in the blockchain; and 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.

13. The apparatus according to claim 12, wherein the auxiliary information comprises any one of or a combination of at least two of the following:

- an identifier of a data uploader;
- an upload timestamp of the target data; or
- an upload location of the target data.

14. The apparatus according to claim 8, wherein the second acquisition module 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.

15. An electronic device, comprising:

a processor; and

a memory, configured to store machine executable instructions; wherein

by reading and executing the machine executable instructions that are stored in the memory and that correspond to a control logic for blockchain-based data verification, the processor is enabled to:

obtain 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;

determine whether the target data has been stored in the blockchain based on the data identifier;

if it is 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;

if the target data has been stored in the blockchain, obtain the target data from the storage location indicated by the data identifier, wherein the target data stored in the blockchain carries verification information used to verify authenticity of the target data, wherein the verification information is a hash value obtained by performing a hash calculation based on original content of the target data and auxiliary information;

verify authenticity of the obtained target data based on the verification information; and
output a verification result to a data verifier.