

Claims

1. A data storage method, wherein the method comprises:

determining a first check value of a first data version of a target object;

searching for a second check value of a second data version of the target object that
5 is adjacent to the first data version;

creating a data block based on the first check value and the second check value and
storing the data block in a blockchain, wherein the data block stored in the blockchain is
immutable.

2. The data storage method according to claim 1, wherein the determining a first
10 check value of a first data version of a target object comprises:

determining a data content summary of the target object in the first data version;

calculating the first check value of the first data version of the target object
according to a preset algorithm and the data content summary.

3. The data storage method according to claim 1, wherein the creating a data
15 block based on the first check value and the second check value comprises:

creating the data block, and writing the first check value and the second check value
in a data header of the data block according to a preset format.

4. The data storage method according to claim 3, wherein the method further
comprises:

20 writing a data content summary of the target object in the first data version, or the
second check value, or data content of the first data version of the target object in a data
body of the data block.

5. The data storage method according to claim 3, wherein the method further
comprises:

25 storing data content of the first data version of the target object in a cloud data
gateway or a database.

6. The data storage method according to claim 1, wherein after storing the data
block in the blockchain, the method further comprises:

storing a mapping relationship between a version identifier of the first data version of the target object and a block identifier of the data block.

7. The data storage method according to any of the claims 1 to 6, wherein the storing the data block in a blockchain comprises:

5 according to a linked data structure, adding the data block to the blockchain.

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

receiving a data authentication request, the data authentication request comprising a version identifier of the first data version of the target object and a third check value obtained based on data content of the target object;

10 based on the version identifier in the data authentication request, searching, in the blockchain, for the first check value;

based on the third check value and the first check value, authenticating the data content of the target object.

15 9. The method according to claim 8, wherein the based on the third check value and the first check value, authenticating the data content of the target object comprises:

when the third check value is the same as the first check value, determining that the data content of the target object is authentic;

when the third check value is different from the first check value, determining that the data content of the target object has been modified.

20 10. The method according to claim 8 or claim 9, wherein the based on the version identifier in the data authentication request, searching, in the blockchain, for the first check value comprises:

25 based on pre-stored mapping relationships between version identifiers of data versions and block identifiers of data blocks, determining a block identifier corresponding to the version identifier in the data authentication request;

reading the first check value from the blockchain based on the block identifier.

11. A data tracing method, wherein the method comprises:

receiving a data backtracking request, the data backtracking request comprising a version identifier of a first data version of the data to be backtracked;

based on the version identifier of the first data version, searching, in a blockchain, for a data block containing the version identifier of the first data version, and obtaining, from the data block, a version identifier of a second data version adjacent to the first data version;

- 5 based on the obtained version identifier of the second data version, backtracking sequentially to obtain a data block containing the version identifier of the initial version of the data to be backtracked;

based on the data block, determining data content corresponding to the initial version of the data to be backtracked.

- 10 12. The data tracing method according to claim 11, wherein the based on the obtained version identifier of the second data version, backtracking sequentially to obtain a data block containing the version identifier of the initial version of the data to be backtracked comprises:

- 15 based on an obtained version identifier of a data version, executing the following operation until a data block containing the version identifier of the initial version of the data to be backtracked is obtained:

searching, in the blockchain, for a data block containing the obtained version identifier of the data version, and obtaining from the data block a version identifier of a previous data version adjacent to the obtained data version;

- 20 triggering cyclic execution of the foregoing operations until a data block containing the version identifier of the initial version of the data to be backtracked is obtained.

13. A data storage apparatus, wherein the apparatus comprises:

a determining module determining a first check value of a first data version of a target object;

- 25 a searching unit searching for a second check value of a second data version of the target object that is adjacent to the first data version;

a storage module creating a data block based on the first check value and the second check value and storing the data block in a blockchain, wherein the data block stored in the blockchain is immutable.

- 30 14. The data storage apparatus according to claim 13, wherein the determining module determining a first check value of a first data version of a target object comprises:

determining a data content summary of the target object in the first data version;
 calculating the first check value of the first data version of the target object
 according to a preset algorithm and the data content summary.

15. The data storage apparatus according to claim 13, wherein the storage module
 5 creating a data block based on the first check value and the second check value comprises:
 creating the data block, and writing the first check value and the second check value
 in a data header of the data block according to a preset format.

16. The data storage apparatus according to claim 15, wherein the data storage
 apparatus further comprises: a writing module, wherein:

10 the writing module writes a data content summary of the target object in the first
 data version, or the second check value, or data content of the first data version of the
 target object in a data body of the data block.

17. The data storage apparatus according to claim 15, wherein
 the storage module stores data content of the first data version of the target object in
 15 a cloud data gateway or a database.

18. The data storage apparatus according to claim 13, wherein
 the storage module, after storing the data block in the blockchain, stores a mapping
 relationship between a version identifier of the first data version of the target object and a
 block identifier of the data block.

19. The data storage apparatus according to any of the claims 13 to 18, wherein
 20 the storage module storing the data block in a blockchain comprises:

according to a linked data structure, adding the data block to the blockchain.

20. The apparatus according to claim 13, wherein the apparatus further comprises:
 a receiving module receiving a data authentication request, the data authentication
 25 request comprising a version identifier of the first data version of the target object and a
 check value obtained based on data content of the target object;

a searching module searching, in the blockchain, based on the version identifier in
 the data authentication request, for the first check value;

an authenticating module authenticating the data content of the target object based on the received check value contained in the data authentication request and the first check value.

21. The apparatus according to claim 20, wherein the authenticating module
5 authenticating the data content of the target object based on the received check value contained in the data authentication request and the first check value comprises:

when the received check value contained in the data authentication request is the same as the first check value, determining that the data content of the target object is authentic;

10 when the received check value contained in the data authentication request is different from the first check value, determining that the data content of the target object has been modified.

22. The apparatus according to claim 20 or claim 21, wherein the searching module searching, in the blockchain, based on the version identifier in the data
15 authentication request, for the first check value comprises:

based on pre-stored mapping relationships between version identifiers of a data versions and block identifiers of a data blocks, determining a block identifier corresponding to the version identifier in the data authentication request,

reading the first check value from the blockchain based on the block identifier.

20 23. A data tracing apparatus, wherein the apparatus comprises:

a receiving module receiving a data backtracking request, the data backtracking request comprising a version identifier of a first data version of the data to be backtracked;

a backtracking module searching, in a blockchain, based on the version identifier of the first data version, for a data block containing the version identifier of the first data
25 version, and obtaining, from the data block, a version identifier of a second data version adjacent to the first data version; based on the obtained version identifier of the second data version, backtracking sequentially to obtain a data block containing the version identifier of the initial version of the data to be backtracked;

a determining module determining data content corresponding to the initial version
30 of the data to be backtracked based on the data block.

24. The data tracing apparatus according to claim 23, wherein the backtracking module, based on the obtained version identifier of the second data version, backtracking sequentially to obtain a data block containing the version identifier of the initial version of the data to be backtracked comprises:

5 based on an obtained version identifier of a data version, executing the following operation until a data block containing the version identifier of the initial version of the data to be backtracked is obtained:

 searching, in the blockchain, for a data block containing the obtained version identifier of the data version, and obtaining from the data block a version identifier of a
10 previous data version adjacent to the obtained data version;

 triggering cyclic execution of the foregoing operations until a data block containing the version identifier of the initial version of the data to be backtracked is obtained.