

What is claimed is:

1. An information authentication method, comprising:

generating first transaction information based on content information of first information to be published by an original information publishing end and a HASH value of the first information, wherein the first information is original information or a copy of the original information, the first transaction information comprises the content information of the first information and the HASH value of the first information, and the original information publishing end is news media or a website;

writing content information except an ID of information in the content information of the first information into a central database and writing the HASH value of the first information and the ID of information into a Blockchain, or writing the content information of the first information and the HASH value of the first information into the Blockchain;

obtaining reprinted information published by an information reprinting end, and generating a HASH value of the reprinted information;

comparing the HASH value of the first information written into the Blockchain with the HASH value of the reprinted information; and

returning a first credential, which indicates the reprinted information is true or has not been tampered with, to the information reprinting end, if the HASH value of the first information is equal to the HASH value of the reprinted information.

2. The information authentication method according to claim 1, before generating first transaction information based on content information of first information to be published by an original information publishing end and a HASH value of the first information, the method further comprises:

obtaining the first information to be published by the original information publishing end;

extracting the content information of the first information; and

generating the HASH value of the first information,

wherein the information authentication method further comprises:

returning a second credential, which indicates the reprinted information is untrue or has been tampered with, to the information reprinting end, or skipping returning any credential, if the HASH value of the first information is unequal to the HASH value of the reprinted information.

3. The information authentication method according to claim 1 or 2, wherein the obtaining reprinted information published by an information reprinting end, and generating a HASH value

of the reprinted information further comprises:

extracting content information of the reprinted information based on the reprinted information ,

5 wherein after the generating a HASH value of the reprinted information, the information authentication method further comprises:

generating second transaction information from the HASH value of the reprinted information and the content information of the reprinted information;

writing the second transaction information into the central database and the Blockchain, or into the Blockchain.

10 4. The information authentication method according to claim 3, wherein writing entire content of the second transaction information into the Blockchain, when writing the second transaction information into the Blockchain;

writing entire content of the second transaction information into the central database and writing a HASH value in the second transaction information and an ID in the second transaction
15 information into the Blockchain, when writing the second transaction information into the Blockchain and the central database.

5. The information authentication method according to claim 3 or 4, wherein the second transaction information further comprises a HASH value of a parent transaction of the reprinted information.

20 6. The information authentication method according to any one of claims 1 to 5, further comprising:

extracting, from the central data base or the Blockchain, the first transaction information of the first information corresponding to the reprinted information, when the first credential is accessed.

25 7. The information authentication method according to any one of claims 1 to 6, further comprising:

obtaining terminal information from an information reading end, and generating a HASH value of the terminal information;

30 comparing the HASH value of the terminal information with the HASH value of the first information; and

returning a third credential, which indicates the terminal information is true or has not been tampered with, to the information reading end, if the HASH value of the terminal

information is equal to the HASH value of the first information.

8. The information authentication method according to claim 7, further comprising:

returning a fourth credential, which indicates the terminal information is untrue or has been tampered with, to the information reading end, or skipping returning any credential, if the
5 HASH value of the terminal information is unequal to the HASH value of the first information.

9. The information authentication method according to claim 7 or 8, further comprising:

extracting, from the central database or the Blockchain, the second transaction information of the reprinted information corresponding to the terminal information, when the third credential is accessed.

10. The information authentication method according to any one of claims 7 to 9, wherein the first credential and the third credential are represented as a two-dimensional code.

11. The information authentication method according to any one of claims 1 to 10, wherein except the ID of information in the content information of the first information, the content information of the first information further comprises: at least one of a title of the information,
15 a content of the information, an author of the information, a date of the information, and a posting site name of the information.

12. An information authentication system, comprising:

an generating module, configured to generate first transaction information based on content information of first information to be published by an original information publishing
20 end and a HASH value of the first information, wherein the first information is original information or a copy of the original information, the first transaction information comprises the content information of the first information and the HASH value of the first information, and the original information publishing end is news media or a website;

a writing module, configured to write content information except an ID of information in
25 the content information of the first information into a central database and writing the HASH value of the first information and the ID of information into a Blockchain, or writing the content information of the first information and the HASH value of the first information into the Blockchain;

an obtaining module, configured to obtain reprinted information published by an
30 information reprinting end, and generate a HASH value of the reprinted information;

a comparing module, configured to compare the HASH value of the first information written into the Blockchain with the HASH value of the reprinted information; and

a returning module, configured to return a first credential, which indicates the reprinted

information is true or has not been tampered with, to the information reprinting end, if the HASH value of the first information is equal to the HASH value of the reprinted information.

13. The information authentication system according to claim 12, wherein the obtaining module is further configured to obtain the first information to be published by the original information publishing end, extract the content information of the first information, and generate the HASH value of the first information,

wherein the returning module is further configured to return a second credential, which indicates the reprinted information is untrue or has been tampered with, to the information reprinting end, or skip returning any credential, if the HASH value of the first information is unequal to the HASH value of the reprinted information.

14. The information authentication system according to claim 12 or 13, wherein the obtaining module is further configured to extract content information of the reprinted information based on the reprinted information;

the generating module is further configured to generate second transaction information from the HASH value of the reprinted information and the content information of the reprinted information; and

the writing module is further configured to write the second transaction information into the central database and the Blockchain, or into the Blockchain.

15. The information authentication system according to claim 14, wherein the writing module is configured to write entire content of the second transaction information into the Blockchain, when writing the second transaction information into the Blockchain;

the writing module is configured to write entire content of the second transaction information into the central database and write a HASH value in the second transaction information and an ID in the second transaction information into the Blockchain, when writing the second transaction information into the Blockchain and the central database.

16. The information authentication system according to claim 14 or 15, wherein the second transaction information further comprises a HASH value of a parent transaction of the reprinted information.

17. The information authentication system according to any one of claims 12 to 16, further comprising:

the extracting module is configured to extract, from the central data base or the Blockchain, the first transaction information of the first information corresponding to the reprinted information, when the first credential is accessed.

18. The information authentication system according to any one of claims 12 to 17, wherein the obtaining module is further configured to obtain terminal information from an information reading end, and generate a HASH value of the terminal information;

the comparing module is further configured to compare the HASH value of the terminal information with the HASH of the first information; and

the returning module is further configured to return a third credential, which indicates the terminal information is true or has not been tampered with, to the information reading end, if the HASH value of the terminal information is equal to the HASH value of the first information.

19. The information authentication system according to claim 18, wherein the returning module is further configured to return a fourth credential, which indicates the terminal information is untrue or has been tampered with, to the information reading end, or skip returning any credential, if the HASH value of the terminal information is unequal to the HASH value of the first information.

20. The information authentication system according to claim 18 or 19, wherein the extracting module is further configured to extract, from the central database or the Blockchain, the second transaction information of the reprinted information corresponding to the terminal information, when the third credential is accessed.

21. The information authentication system according to any one of claims 18 to 20, wherein the first credential and the third credential are represented as a two-dimensional code.

22. The information authentication system according to any one of claims 12 to 21, wherein except the ID of information in the content information of the first information, the content information of the first information further comprises at least one of a title of the information, a content of the information, an author of the information, a date of the information, and a posting site name of the information.

23. A computer device, comprising:

a processor; and

a memory storing a computer program that, when executed by the processor, causes the processor to perform the information authentication method according to any one of claims 1 to 11.

24. A computer readable storage medium storing a computer program that, when executed by a processor, causes the processor to perform the information authentication method according to any one of claims 1 to 11.