

CLAIMS

1. A computer-implemented method for maintaining data, comprising:
receiving, by a service computer system, data from a client device;
generating, by the service computer system, ledger data based on the data;
sending, by the service computer system, the ledger data to a blockchain-based trusted system;
receiving, by the service computer system, a credential corresponding to the ledger data from the blockchain-based trusted system; and
sending, by the service computer system, the credential to the client device.
2. The computer-implemented method of claim 1, further comprising:
receiving, by the service computer system from the client device, a request to store the data, the request comprising the data.
3. The computer-implemented method of any preceding claim, further comprising:
after receiving the data from the client device, storing, by the service computer system, the data in a local storage of the service computer system.
4. The computer-implemented method of any preceding claim, further comprising:
after generating the ledger data, sending, by the service computer system to the blockchain-based trusted system, a request to store the ledger data.
5. The computer-implemented method of any preceding claim, wherein generating the ledger data based on the data comprises:
computing, by the service computing system, a hash value of the data; and
generating, by the service computing system, the ledger data comprising the hash value.
6. The computer-implemented method of any preceding claim, wherein the ledger data further comprises metadata of the data.
7. The computer-implemented method of any preceding claim, further comprising:

receiving, by the blockchain-based trusted system, the ledger data from the service computer system;

storing, by the blockchain-based trusted system, the ledger data in the blockchain-based trusted system;

generating, by the blockchain-based trusted system, the credential corresponding to the ledger data; and

sending, by the blockchain-based trusted system to the service computer system, the credential corresponding to the ledger data.

8. The computer-implemented method of any preceding claim, wherein the credential corresponding to the ledger data comprises an identifier of the ledger data or a digital signature of the blockchain-based trusted system.

9. The computer-implemented method of any preceding claim, wherein the hash value is a first hash value, and the method further comprising:

after storing the data in the local storage, receiving, by the service computer system, a request to verify the data;

obtaining, by the service computer system, the data from the local storage;

computing, by the service computer system, a second hash value based on the data obtained from the local storage;

sending, by the service computer system to the blockchain-based trusted system, a request that comprises the second hash value for verifying the second hash value; and

receiving, by the service computer system, a verification result from the blockchain-based trusted system, wherein the verification result comprises a comparison result of the first hash value and the second hash value.

10. The computer-implemented method of any preceding claim, wherein the request to verify the data comprises the credential.

11. The computer-implemented method of any preceding claim, further comprising:

after receiving the verification result from the blockchain-based trusted system, determining, by the service computer system, whether the first hash value matches the second hash value based on the verification result.

12. The computer-implemented method of any preceding claim, further comprising:

in response to determining that the first hash value matches the second hash value based on the verification result, sending, by the service computer system to the client device, a notification indicating that the data has not been tampered with.

13. The computer-implemented method of any preceding claim, further comprising:

in response to determining that the first hash value does not match the second hash value based on the verification result, sending, by the service computer system to the client device, a notification indicating that the data has been tampered with.

14. A system for maintaining data, comprising:

one or more processors; and

one or more computer-readable memories coupled to the one or more processors and having instructions stored thereon that are executable by the one or more processors to perform the method of any of claims 1 to 13.

15. An apparatus for maintaining data, the apparatus comprising a plurality of modules for performing the method of any of claims 1 to 13.