

CLAIMS

1. A computer-implemented method performed by a blockchain-based trusted platform, the computer-implemented method comprises:

- receiving, from a client device and via a recording input interface, first ledger data to be recorded on a blockchain;

- determining whether original ledger data associated with the first ledger data satisfies a recording rule, wherein the recording rule comprises one or more recording input parameters associated with the recording input interface;

- in response to determining that the original ledger data associated with the first ledger data satisfies the recording rule, recording the original ledger data on the blockchain;

- generating a recording receipt associated with the first ledger data; and

- transmitting, to the client device and via a recording output interface, the recording receipt, wherein the method further comprises:

- receiving, from the client device and via a verification input interface, second ledger data;

- determining whether the second ledger data satisfies a verification rule, wherein the verification rule comprises one or more verification input parameters associated with the verification input interface;

- in response to determining that the second ledger data satisfies the verification rule, determining whether the second ledger data corresponds to the original ledger data recorded on the blockchain;

- in response to determining that the second ledger data corresponds to the original ledger data recorded on the blockchain, generating a verification receipt associated with the second ledger data, wherein the verification receipt indicates that raw data associated with the second ledger data is not tampered with; and

- transmitting, to the client device and via a verification output interface, the verification receipt.

2. The computer-implemented method of any preceding claim, wherein determining whether the second ledger data corresponds to the original ledger data comprises determining

whether a first hash value comprised in the original ledger data matches a second hash value comprised in the second ledger data.

3. The computer-implemented method of any preceding claim, wherein the first ledger data comprises a bit stream, wherein before receiving the first ledger data, the client device converts the original ledger data to the bit stream based on a conversion rule, and wherein the computer-implemented method further comprises:

converting, based on the conversion rule, the bit stream to obtain the original ledger data.

4. The computer-implemented method of any preceding claim, wherein the conversion rule comprises at least one of:

a coding scheme corresponding to each recording input parameter of the one or more recording input parameters; or

an order to arrange the one or more recording input parameters in the bit stream.

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

invoking a trusted timing module to generate a first recording timestamp representing a time that the first ledger data is received;

invoking a trusted identity module to verify a user identity associated with the client device;

invoking the trusted timing module to generate a second recording timestamp representing a time that the original ledger data is recorded on the blockchain; and

invoking a trusted computing module to generate a blockchain transaction comprising the original ledger data, the user identity, the first recording timestamp, and the second recording timestamp.

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

before receiving the first ledger data, establishing a secure communication channel with the client device based on at least one of a two-way transport layer security (TLS) protocol, a two-way hypertext transfer protocol secure (HTTPS) protocol, or a one-way HTTPS protocol.

7. The computer-implemented method of any preceding claim, wherein the first ledger data is associated with a first data file, and wherein the one or more recording input parameters comprise one or more of a hash value of the first data file, attribute information of the first data file, service information of the first data file, a timestamp of the first data file, and signature data of the first data file.

8. The computer-implemented method of any preceding claim, wherein the second ledger data is associated with a second data file, and wherein the one or more verification input parameters comprise one or more of a hash value of the second data file, service information of the second data file, a timestamp of the second data file, and signature data of the second data file.

9. The computer-implemented method of any preceding claim, wherein the client device is associated with an additional blockchain that is different from the blockchain.

10. A computer-implemented system, comprising:

- at least one processor; and

- a non-transitory computer-readable storage medium coupled to the at least one processor and storing programming instructions for execution by the at least one processor, the programming instructions instruct the at least one processor to perform operations comprising:

- executing a data recording function to record ledger data on a blockchain;

- executing a data verification function to verify ledger data recorded on the blockchain;

- invoking a trusted service layer to provide trusted computations for executing the data recordation function and the data verification function; and

- invoking a blockchain layer to interface the data recording function with the blockchain, wherein the blockchain layer comprises a recording input interface and a recording output interface, and wherein the data recording function is configured to:

- receive, from a client device and via the recording input interface, first ledger data to be recorded on the blockchain;

determine whether original ledger data associated with the first ledger data satisfies a recording rule, wherein the recording rule comprises one or more recording input parameters associated with the recording input interface;

in response to determining that the original ledger data associated with the first ledger data satisfies the recording rule, record the original ledger data on the blockchain;

generate a recording receipt associated with the first ledger data; and

transmit, to the client device and via the recording output interface, the recording receipt, wherein the blockchain layer comprises a verification input interface and a verification output interface, wherein the data verification function is configured to:

receive, from the client device and via the verification input interface, second ledger data;

determine whether the second ledger data satisfies a verification rule, wherein the verification rule comprises one or more verification input parameters associated with the verification input interface;

in response to determining that the second ledger data satisfies the verification rule, determine whether the second ledger data corresponds to the original ledger data recorded on the blockchain;

in response to determining that the second ledger data corresponds to the original ledger data recorded on the blockchain, generate a verification receipt associated with the second ledger data, wherein the verification receipt indicates that raw data associated with the second ledger data is not tampered with; and

transmit, to the client device and via the verification output interface, the verification receipt.

11. The computer-implemented system of claim 10, wherein determining whether the second ledger data corresponds to the original ledger data comprises determining whether a first hash value comprised in the original ledger data matches a second hash value comprised in the second ledger data.

12. The computer-implemented system of any of claims 10 to 11, wherein the first ledger data comprises a bit stream, wherein, before receiving the first ledger data, the client device converts the original ledger data to the bit stream based on a conversion rule, and wherein the data recording function is further configured to:

convert, based on the conversion rule, the bit stream to obtain the original ledger data.

13. The computer-implemented system of any of claims 10 to 12, wherein the conversion rule comprises at least one of:

a coding scheme corresponding to each recording input parameter of the one or more recording input parameters; or

an order to arrange the one or more recording input parameters in the bit stream.

14. The computer-implemented system of any of claims 10 to 13, wherein the trusted service layer comprises a trusted timing module, a trusted identity module, and a trusted computing module, and the data recording function is further configured to:

invoke the trusted timing module to generate a first recording timestamp representing a time that the first ledger data is received by the data recording function;

invoke the trusted identity module to verify a user identity associated with the client device;

invoke the trusted timing module to generate a second recording timestamp representing a time that the original ledger data is recorded on the blockchain; and

invoke the trusted computing module to generate a blockchain transaction comprising the original ledger data, the user identity, the first recording timestamp, and the second recording timestamp.

15. The computer-implemented system of any of claims 10 to 14, wherein the data recording function is further configured to:

before receiving the first ledger data, establish a secure communication channel with the client device based on at least one of a two-way transport layer security (TLS) protocol, a two-way hypertext transfer protocol secure (HTTPS) protocol, or a one-way HTTPS protocol.

16. The computer-implemented system of any of claims 10 to 15, wherein the first ledger data is associated with a first data file, and wherein the one or more recording input parameters comprise one or more of a hash value of the first data file, attribute information of the first data file, service information of the first data file, a timestamp of the first data file, and signature data of the first data file.

17. The computer-implemented system of any of claims 10 to 16, wherein the second ledger data is associated with a second data file, and wherein the one or more verification input parameters comprise one or more of a hash value of the second data file, service information of the second data file, a timestamp of the second data file, and signature data of the second data file.

18. The computer-implemented system of any of claims 10 to 17, wherein the client device is associated with an additional blockchain that is different from the blockchain.

19. An apparatus, the apparatus comprising a plurality of modules for performing the method of any of claims 1 to 9.