

Claims:

1. A smart contract-based data transfer method, comprising the steps of:

a) a data source encrypting data to be transferred based on a first mechanism to form encrypted data, and sending the encrypted data to a smart contract terminal;

b) the smart contract terminal decrypting the encrypted data based on a second mechanism corresponding to the first mechanism to form the decrypted data, and processing the decrypted data by using at least one logic unit to form the resulting data; and

c) the smart contract terminal sending the resulting data to a data-related party;

wherein the at least one logic unit executes an instruction set to implement a contract logic, and the instruction set is stored in a blockchain, the resulting data has no correlation with the data to be transferred, and the instruction set comprises:

a first instruction, executed to implement a training logic based on a first portion of the decrypted data, wherein the training logic is configured to train a prediction model;

a second instruction, executed to implement a prediction logic based on a second portion of the decrypted data, wherein the prediction logic is configured to use the prediction model to output a prediction result.

2. The method of claim 1, wherein the at least one logic unit comprises:

a first logic unit, configured to execute the instruction to implement a first logic;

a second logic unit, configured to execute the instruction to implement a second logic; and

a third logic unit, configured to combine the first logic with the second logic to output the resulting data.

3. The method according to claim 1, wherein:

the first mechanism comprises a public key, wherein the public key is generated by the smart contract terminal in response to a request from the data source to the smart contract terminal and issued to the data source;

the second mechanism comprises a private key, wherein the private key is generated by the smart contract terminal in the manner that the private key is paired with the public key.

4. The method of claim 1, wherein:

the step a) further comprises:

the smart contract terminal requiring the data source to provide a first digital certificate for verifying the data source;

the step c) further comprises:

the smart contract terminal requiring the data-related party to provide a second digital certificate for verifying the data-related party.

5. A smart contract-based data transfer system, comprising:

a data source, configured to encrypt data to be transferred based on a first mechanism to form encrypted data, and send the encrypted data to a smart contract terminal;

the smart contract terminal, configured to decrypt the encrypted data based on a second mechanism corresponding to the first mechanism to form the decrypted data, and process the decrypted data by using at least one logic unit to form the resulting data; and

a data-related party, configured to receive the resulting data from the smart contract terminal;

wherein the smart contract terminal comprises at least one logic unit, configured to execute an instruction set to implement a contract logic, and wherein the instruction set is stored in a blockchain, the resulting data has no correlation with the data to be transferred, and the instruction set comprises:

a first instruction, executed to implement a training logic based on a first portion of the decrypted data; wherein the training logic is configured to train a prediction model;

a second instruction, executed to implement a prediction logic based on a second portion of the decrypted data; wherein the prediction logic is configured to use the prediction model to output a prediction result.

6. The system of claim 5 wherein the at least one logic unit comprises:

a first logic unit, configured to execute the instruction to implement a first logic;

a second logic unit, configured to execute the instruction to implement a second logic;
and

a third logic unit, configured to combine the first logic with the second logic to output the resulting data.

7. The system of claim 5, wherein:

the first mechanism comprises a public key, wherein the public key is generated by the smart contract terminal in response to a request from the data source to the smart contract terminal and issued to the data source;

the second mechanism comprises a private key, wherein the private key is generated by the smart contract terminal in the manner that the private key is paired with the public key.

8. The system of claim 5, wherein the system is deployed on the basis of a distributed system.

9. A computer storage medium for storing computer-executable instructions, wherein the computer-executable instructions are configured to, when executed by a processor, perform steps of:

a) a data source encrypting data to be transferred based on a first mechanism to form encrypted data, and sending the encrypted data to a smart contract terminal;

b) the smart contract terminal decrypting the encrypted data based on a second mechanism corresponding to the first mechanism to form the decrypted data, and processing the decrypted data by using at least one logic unit to form the resulting data; and

c) the smart contract terminal sending the resulting data to a data-related party;

wherein the at least one logic unit executes an instruction set to implement a contract logic, and the instruction set is stored in a blockchain, the resulting data has no correlation with the data to be transferred, and the instruction set comprises:

a first instruction, executed to implement a training logic based on a first portion of the decrypted data, wherein the training logic is configured to train a prediction model;

a second instruction, executed to implement a prediction logic based on a second portion of the decrypted data, wherein the prediction logic is configured to use the prediction model to output a prediction result.

10. The system of claim 6, wherein the system is deployed on the basis of a distributed system.

11. The system of claim 7, wherein the system is deployed on the basis of a distributed system.

12. A non-transitory computer storage medium for storing computer-executable instructions of claim 9, wherein the at least one logic unit comprises:

a first logic unit, configured to execute the instruction to implement a first logic;

a second logic unit, configured to execute the instruction to implement a second logic;

and

a third logic unit, configured to combine the first logic with the second logic to output the resulting data.

13. A non-transitory computer storage medium for storing computer-executable instructions of claim 9, wherein:

the first mechanism comprises a public key, wherein the public key is generated by the smart contract terminal in response to a request from the data source to the smart contract terminal and issued to the data source;

the second mechanism comprises a private key, wherein the private key is generated by the smart contract terminal in the manner that the private key is paired with the public key.

14. A non-transitory computer storage medium for storing computer-executable instructions of claim 9, wherein:

the step a) further comprises;

the smart contract terminal requiring the data source to provide a first digital certificate for verifying the data source;

the step c) further comprises;

the smart contract terminal requiring the data-related party to provide a second digital certificate for verifying the data-related party.