CLAIMS

What is claimed is:

1. A service processing method, applied to a node device accessed to a blockchain, comprising:

receiving a message processing request sent by a channel partner device, wherein the message processing request comprises at least one message ciphertext to be processed, and the message processing request further comprises identifier information of a service provider corresponding to the service provider device;

invoking a first smart contract deployed in the blockchain from a TEE of the node device, and decrypting the message ciphertext based on the first smart contract to obtain the message plaintext, wherein the decrypting comprises:

obtaining associated decryption information from a predetermined association relationship between the identifier information and the decryption information based on the first smart contract and the identifier information; and

decrypting the message ciphertext based on the obtained decryption information to obtain the message plaintext; and

sending the message plaintext to an operator device so that the operator device sends the message to be sent in the message plaintext to the target user.

2. The method according to claim 1, wherein the receiving a message processing request sent by a channel partner device comprises:

receiving, through a first trusted application in the node device, the message processing request sent by a second trusted application in the channel partner device, wherein the first trusted application and the second trusted application are related to message processing; and

the sending the message plaintext to an operator device comprises:

sending the message plaintext to the operator device through the first trusted application.

3. The method according to claim 2, wherein the first trusted application is set in the TEE of the node device; and

the invoking a first smart contract deployed in the blockchain from a TEE of the node device comprises:

invoking the first smart contract deployed in the blockchain through the first trusted application.

4. The method according to claim 2, wherein the first trusted application is set outside the TEE of the node device;

the invoking a first smart contract deployed in the blockchain from a TEE of the node device comprises:

transmitting the message ciphertext to the TEE of the node device through the first trusted application; and

invoking the first smart contract deployed in the blockchain from the TEE of the node device; and

the sending the message plaintext to the operator device through the first trusted application comprises:

obtaining the message plaintext from the TEE of the node device through the first trusted application, and sending the obtained message plaintext to the operator device.

5. The method according to claim 2, wherein the first trusted application comprises a trusted side program set in the TEE of the node device, and a client program set outside the TEE of the node device;

the receiving, through the first trusted application in the node device, the message processing request sent by a second trusted application in the channel partner device comprises:

receiving, through the client program in the node device, the message processing request sent by the second trusted application in the channel partner device;

the invoking a first smart contract deployed in the blockchain from a TEE of the node device comprises:

transmitting the message ciphertext to the trusted side program through the client program, and

invoking the first smart contract deployed in the blockchain through the trusted side program; and

the sending the message plaintext to the operator device through the first trusted application comprises:

obtaining the message plaintext from the trusted side program through the client program, and sending the obtained message plaintext to the operator device.

6. The method according to claim 1, wherein the sending the message plaintext to an operator device so that the operator device sends the message to be sent in the message plaintext to the target user comprises:

determining a target operator device corresponding to each message plaintext; and

sending the message plaintext to the corresponding target operator device so that the target operator device sends the message to be sent in the message plaintext to the target user.

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

receiving service processing record information sent by the service provider device, and storing the service processing record information to the blockchain, wherein the service processing record information is generated by the service provider device based on the message ciphertext and service identifier information comprised in the service processing request;

receiving a service query request sent by a querier device, wherein the service query request comprises service identifier information of a service to be queried;

querying associated service processing record information from the blockchain based on the service identifier information; and

sending query result information to the querier device based on the queried service processing record information.

8. A service processing apparatus, applied to a node device accessed to a blockchain, comprising:

a receiving module, configured to receive a message processing request sent by a channel partner device, wherein the message processing request comprises at least one message ciphertext to be processed, and the message processing request further comprises identifier information of a service provider corresponding to the service provider device;

a decryption module, configured to invoke a first smart contract deployed in the blockchain from a TEE of the node device, obtain associated decryption information from a predetermined association relationship between the identifier information and the decryption information based on the first smart contract and the identifier information, and decrypt the message ciphertext based on the obtained decryption information to obtain the message plaintext; and

a sending module, configured to send the message plaintext to an operator device so that the operator device sends the message to be sent in the message plaintext to the target user.

9. The apparatus according to claim 8, wherein

the receiving module receives the message processing request sent by a second trusted application in the channel partner device through a first trusted application in the node device, wherein the first trusted application and the second trusted application are related to message processing; and

the sending module sends the message plaintext to the operator device through the first trusted application.

10. A service processing system, comprising a service provider device, a channel partner device, an operator device, and a blockchain system, wherein

the channel partner device receives the message ciphertext sent by the service provider device, and sends, based on the message ciphertext, a message processing request to a node device in the blockchain system, wherein the message processing request comprises at least one message ciphertext to be processed and identifier information of a service provider corresponding to the service provider device;

the node device in the blockchain system receives the message processing request sent by the channel partner device, invokes a first smart contract deployed in the blockchain from a TEE of the node device, decrypts, based on the first smart contract, the message ciphertext to obtain the message plaintext, wherein the decrypting comprises obtaining associated decryption information from a predetermined association relationship between the identifier information and the decryption information based on the first smart contract and the identifier information, and decrypting the message ciphertext based on the obtained decryption information to obtain the message plaintext, and sends the message plaintext to the operator device; and

the operator device receives the message plaintext sent by the node device and sends the message to be sent in the message plaintext to the target user.

11. A service processing device, applied to a node device accessed to a blockchain, comprising:

a processor; and

a memory configured to store computer-executable instructions that, when executed, enable the processor to:

receive a message processing request sent by a channel partner device, wherein the message processing request comprises at least one message ciphertext to be processed, and the message processing request further comprises identifier information of a service provider corresponding to the service provider device;

invoke a first smart contract deployed in the blockchain from a TEE of the node device, obtain associated decryption information from a predetermined association relationship between the identifier information and the decryption information based on the first smart contract and the identifier information, and decrypt the message ciphertext based on the obtained decryption information to obtain the message plaintext; and

send the message plaintext to an operator device so that the operator device sends the message to be sent in the message plaintext to the target user.

12. A storage medium, configured to store computer-executable instructions that, when executed by a processor, implement the following procedure:

receiving a message processing request sent by a channel partner device, wherein the message processing request comprises at least one message ciphertext to be processed, and the message processing request further comprises identifier information of a service provider corresponding to the service provider device;

invoking a first smart contract deployed in a blockchain from a TEE of a node device, and decrypting the message ciphertext based on the first smart contract to obtain the message plaintext, wherein the decrypting comprises:

obtaining associated decryption information from a predetermined association relationship between the identifier information and the decryption information based on the first smart contract and the identifier information; and

decrypting the message ciphertext based on the obtained decryption information to obtain the message plaintext; and

sending the message plaintext to an operator device so that the operator device sends the message to be sent in the message plaintext to the target user.