CLAIMS

What is claimed is:

1. A computer-implemented method, comprising:

receiving, by a trusted execution environment (TEE) deployed in a blockchain and implemented based on CPU hardware and fully isolated from the outside, a user verification result acquisition request from a first institution, wherein the user verification result acquisition request is configured to request a verification result associated with a user and comprises user identity information of the user;

sending, by the TEE deployed in the blockchain, the user verification result acquisition request to the second institution;

receiving, by the TEE, first encrypted data of the user corresponding to the user identity information and sent by the second institution;

decrypting, by the TEE, the first encrypted data to obtain first data of the user;

receiving, by the TEE, second encrypted data of the user corresponding to the user identity information from a third institution, wherein the third institution is a trustworthy institution;

decrypting, by the TEE, the second encrypted data of the user to obtain second data of the user;

in response to the user verification result acquisition request, determining, by the TEE, the verification result of the user, wherein the verification result is obtained by performing matching verification on the first data and the second data and indicates whether the first data matches the second data;

sending, by the TEE, the verification result of the user to the first institution; and

sending, by the TEE, a proof of the verification result to the blockchain.

2. The computer-implemented method of claim 1, wherein the user identity information is identity information of the user that is sent by the second institution to the first institution after the second institution obtains the first data of the user.

3. The computer-implemented method of claim 1, wherein the user identity information comprises a digest value obtained through a hash calculation on one or more pieces of

information of the user.

4. The computer-implemented method of claim 1, wherein the user identity information comprises an account registered by the user at the second institution or an account allocated to the user by a system of the second institution when the user initiates a purchase operation at the second institution.

5. The computer-implemented method of claim 1, wherein determining the verification result of the user comprises:

sending, by the TEE deployed in the blockchain,, the user verification result acquisition request to the second institution;

receiving, by the TEE, the first encrypted data of the user corresponding to the user identity information from the second institution; and

receiving, by the TEE, the second encrypted data of the user corresponding to the user identity information from the third institution, wherein the third institution is a trustworthy institution.

6. The computer-implemented method of claim 5, wherein receiving the user verification result acquisition request from the first institution comprises:

receiving the user verification result acquisition request sent by the first institution by initiation of a first transaction wherein the first transaction is used to invoke a first smart contract deployed on the TEE ; and

in response to the first transaction, invoking, by the TEE, the first smart contract deployed on the TEE.

7. The computer-implemented method of claim 6, wherein sending the user verification result acquisition request to the second institution comprises:

invoking, by the TEE, the first smart contract to send the user verification result acquisition request digitally signed by the TEE to the second institution, or digitally signed by the first smart contract to the second institution; and wherein the proof of the verification result comprises: a verifiable claim signed by the TEE, or a hash value signed by the TEE, wherein the hash value is obtained by performing hash calculation on the verification result.

8. A non-transitory, computer-readable medium storing one or more instructions executable by a computer system to perform operations comprising:

receiving, by a trusted execution environment (TEE) deployed in a blockchain and implemented based on CPU hardware and fully isolated from the outside, a user verification result acquisition request from a first institution, wherein the user verification result acquisition request is configured to request a verification result associated with a user and comprises user identity information of the user;

sending, by the TEE deployed in the blockchain, the user verification result acquisition request to the second institution;

receiving, by the TEE, first encrypted data of the user corresponding to the user identity information and sent by the second institution;

decrypting, by the TEE, the first encrypted data to obtain first data of the user;

receiving, by the TEE, second encrypted data of the user corresponding to the user identity information from a third institution, wherein the third institution is a trustworthy institution;

decrypting, by the TEE, the second encrypted data of the user to obtain second data of the user;

in response to the user verification result acquisition request, determining, by the TEE, the verification result of the user, wherein the verification result is obtained by performing matching verification on the first data and the second data and indicates whether the first data matches the second data;

sending, by the TEE, the verification result of the user to the first institution; and

sending, by the TEE, a proof of the verification result to the blockchain.

9. The non-transitory, computer-readable medium of claim 8, wherein the user identity information is identity information of the user that is sent by the second institution to the first institution after the second institution obtains the first data of the user.

10. The non-transitory, computer-readable medium of claim 8, wherein the user identity information comprises a digest value obtained through a hash calculation on one or more pieces of information of the user.

11. The non-transitory, computer-readable medium of claim 8, wherein the user identity

information comprises an account registered by the user at the second institution or an account allocated to the user by a system of the second institution when the user initiates a purchase operation at the second institution.

12. The non-transitory, computer-readable medium of claim 8, wherein determining the verification result of the user comprises:

sending, by the TEE deployed in the blockchain, the user verification result acquisition request to the second institution;

receiving, by the TEE, the first encrypted data of the user corresponding to the user identity information from the second institution; and

receiving, by the TEE, the second encrypted data of the user corresponding to the user identity information from the third institution, wherein the third institution is a trustworthy institution.

13. The non-transitory, computer-readable medium of claim 12, wherein receiving the user verification result acquisition request from the first institution comprises:

receiving the user verification result acquisition request sent by the first institution by initiation of a first transaction, wherein the first transaction is used to invoke a first smart contract deployed on the TEE; and

in response to the first transaction, invoking, by the TEE, the first smart contract deployed on the TEE.

14. The non-transitory, computer-readable medium of claim 13, wherein sending the user verification result acquisition request to the second institution comprises:

invoking, by the TEE, the first smart contract to send the user verification result acquisition request digitally signed by the TEE to the second institution, or digitally signed by the first smart contract to the second institution; and wherein the proof of the verification result comprises: a verifiable claim signed by the TEE, or a hash value signed by the TEE, wherein the hash value is obtained by performing hash calculation on the verification result.

15. A computer-implemented system, comprising:

one or more computers; and

one or more computer memory devices interoperably coupled with the one or

more computers and having tangible, non-transitory, machine-readable media storing one or more instructions that, when executed by the one or more computers, perform one or more operations comprising:

receiving, by a trusted execution environment (TEE) deployed in a blockchain and implemented based on CPU hardware and fully isolated from the outside, a user verification result acquisition request from a first institution, wherein the user verification result acquisition request is configured to request a verification result associated with a user and comprises user identity information of the user;

sending, by the TEE deployed in the blockchain, the user verification result acquisition request to the second institution;

receiving, by the TEE, first encrypted data of the user corresponding to the user identity information and sent by the second institution;

decrypting, by the TEE, the first encrypted data to obtain first data of the user;

receiving, by the TEE, second encrypted data of the user corresponding to the user identity information from a third institution, wherein the third institution is a trustworthy institution;

decrypting, by the TEE, the second encrypted data of the user to obtain second data of the user;

in response to the user verification result acquisition request, determining, by the TEE, the verification result of the user, wherein the verification result is obtained by performing matching verification on the first data and the second data and indicates whether the first data matches the second data;

sending, by the TEE, the verification result of the user to the first institution; and

sending, by the TEE, a proof of the verification result to the blockchain.

16. The computer-implemented system of claim 15, wherein the user identity information is identity information of the user that is sent by the second institution to the first institution after the second institution obtains the first data of the user.

17. The computer-implemented system of claim 15, wherein the user identity

information comprises a digest value obtained through a hash calculation on one or more pieces of information of the user.

18. The computer-implemented system of claim 15, wherein the user identity information comprises an account registered by the user at the second institution or an account allocated to the user by a system of the second institution when the user initiates a purchase operation at the second institution.

19. The computer-implemented system of claim 15, wherein determining the verification result of the user comprises:

sending, by the TEE deployed in the blockchain, the user verification result acquisition request to the second institution;

receiving, by the TEE, the first encrypted data of the user corresponding to the user identity information from the second institution; and

receiving, by the TEE, the second encrypted data of the user corresponding to the user identity information from the third institution, wherein the third institution is a trustworthy institution.

20. The computer-implemented system of claim 19, wherein receiving the user verification result acquisition request from the first institution comprises:

receiving the user verification result acquisition request sent by the first institution by initiation of a first transaction, wherein the first transaction is used to invoke a first smart contract deployed on the TEE; and

in response to the first transaction, invoking, by the TEE, the first smart contract deployed on the TEE to send the user verification result acquisition request digitally signed by the TEE to the second institution, or digitally signed by the first smart contract to the second institution; and

wherein the proof of the verification result comprises: a verifiable claim signed by the TEE, or a hash value signed by the TEE, wherein the hash value is obtained by performing hash calculation on the verification result.