CLAIMS

What is claimed is:

1. A computer-implemented method, comprising:

receiving, by a trusted execution environment (TEE), 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;

receiving, by the TEE, first encrypted data of the user from a second institution;

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

receiving, by the TEE, second encrypted data of the user from a trusted institution;

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

in response to the user verification result acquisition request, determining, by the TEE, the verification result of the user, wherein the verification result indicates whether the first user basic data matches the second user basic data; and

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

2. The computer-implemented method of claim 1, wherein the first user basic data and the second user basic data comprise user identities comprising at least one of a name of the user, a gender of the user, a phone number of the user, or an address of the user, and wherein the verification result indicates the first user basic data matches the second user basic data if at least one of the user identities comprised in the first user basic data and the second user basic data matches.

3. The computer-implemented method of claim 1, wherein the user verification result acquisition request comprises user identity information of the user, and 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 3, wherein the user identity information comprises an account registered by the user at the second institution or assigned to the user by the second institution in response to an operation initiated by the user at the

second institution.

5. The computer-implemented method of claim 3, wherein determining the verification result of the user comprises:

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

receiving, by the TEE, the first encrypted data from the second institution; and

receiving, by the TEE, the second encrypted data of the user from the trusted institution.

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

initiating, by the TEE, a first transaction to receive the user verification result acquisition request; and

in response to the first transaction, invoking, by the TEE, a 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 smart contract to send the user verification result acquisition request to the second institution.

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), 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;

receiving, by the TEE, first encrypted data of the user from a second institution;

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

receiving, by the TEE, second encrypted data of the user from a trusted institution;

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

in response to the user verification result acquisition request, determining, by

the TEE, the verification result of the user, wherein the verification result indicates whether the first user basic data matches the second user basic data; and

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

9. The non-transitory, computer-readable medium of claim 8, wherein the first user basic data and the second user basic data comprise user identities comprising at least one of a name of the user, a gender of the user, a phone number of the user, or an address of the user, and wherein the verification result indicates the first user basic data matches the second user basic data if at least one of the user identities comprised in the first user basic data and the second user basic data matches.

10. The non-transitory, computer-readable medium of claim 8, wherein the user verification result acquisition request comprises user identity information of the user, and 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 10, wherein the user identity information comprises an account registered by the user at the second institution or assigned to the user by the second institution in response to an operation initiated by the user at the second institution.

12. The non-transitory, computer-readable medium of claim 10, wherein determining the verification result of the user comprises:

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

receiving, by the TEE, the first encrypted data from the second institution; and

receiving, by the TEE, the second encrypted data of the user from the trusted institution.

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

initiating, by the TEE, a first transaction to receive the user verification result acquisition request; and

in response to the first transaction, invoking, by the TEE, a 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 smart contract to send the user verification result acquisition request to the second institution.

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), 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;

receiving, by the TEE, first encrypted data of the user from a second institution;

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

receiving, by the TEE, second encrypted data of the user from a trusted institution;

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

in response to the user verification result acquisition request, determining, by the TEE, the verification result of the user, wherein the verification result indicates whether the first user basic data matches the second user basic data; and

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

16. The computer-implemented system of claim 15, wherein the first user basic data and the second user basic data comprise user identities comprising at least one of a

name of the user, a gender of the user, a phone number of the user, or an address of the user, and wherein the verification result indicates the first user basic data matches the second user basic data if at least one of the user identities comprised in the first user basic data and the second user basic data matches.

17. The computer-implemented system of claim 15, wherein the user verification result acquisition request comprises user identity information of the user, and 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 17, wherein the user identity information comprises an account registered by the user at the second institution or assigned to the user by the second institution in response to an operation initiated by the user at the second institution.

19. The computer-implemented system of claim 17, wherein determining the verification result of the user comprises:

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

receiving, by the TEE, the first encrypted data from the second institution; and

receiving, by the TEE, the second encrypted data of the user from the trusted institution.

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

initiating, by the TEE, a first transaction to receive the user verification result acquisition request; and

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