CLAIMS

What is claimed is:

~~1. An information sharing method, wherein the method is applied to a privacy computing unit and comprises:~~

~~obtaining a user verification result acquisition request sent by a first institution;~~

~~determining a verification result of a user that is requested by the user verification result acquisition request, wherein the verification result is a verification result obtained by performing matching verification on first data and second data; the first data is user basic data obtained by decrypting first encrypted data of the user that is sent by a second institution; the second data is user basic data obtained by decrypting second encrypted data of the user that is sent by a third institution; and the third institution is a trustworthy institution; and~~

~~sending the verification result to the first institution.~~

~~2. The method according to claim 1, wherein the first institution is a financial institution, and the second institution is a sales agency.~~

~~3. The method according to claim 1 or 2, wherein the user verification result acquisition request comprises user identity information of the user.~~

~~4. The method according to claim 3, 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 user basic data of the user.~~

~~5. The method according to claim 3, 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.~~

~~6. The method according to claim 5, wherein the user identity information comprises:~~

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

~~7. The method according to claim 6, wherein the user identity information comprises:~~

~~a digest value obtained through salting hash calculation on one or more pieces of~~

information of the user.

8. The method according to claim 3, wherein the user identity information comprised in the user verification result acquisition request is encrypted.

9. The method according to claim 3, wherein the user verification result acquisition request further comprises a signature of the first institution.

10. The method according to claim 3, wherein the determining a verification result of a user that is requested by the user verification result acquisition request specifically comprises:

determining a verification result of a user corresponding to the user identity information from a pre-generated user verification result, wherein the verification result of the user is a user verification result obtained by performing matching verification on the first data and the second data in advance.

11. The method according to claim 3, wherein the determining a verification result of a user that is requested by the user verification result acquisition request specifically comprises:

sending the user verification result acquisition request to the second institution;

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

obtaining second encrypted data of the user corresponding to the user identity information from the third institution, and decrypting the second encrypted data to obtain the second data of the user; and

performing matching verification on the first data and the second data to obtain the verification result of the user.

12. The method according to claim 11, wherein the sending the user verification result acquisition request to the second institution specifically comprises:

sending the user verification result acquisition request to the second institution by using the privacy computing unit deployed on a blockchain; or

sending the user verification result acquisition request to the second institution by using the privacy computing unit deployed off a blockchain.

13. The method according to claim 11, wherein the obtaining a user verification result acquisition request sent by a first institution specifically comprises:

obtaining a user verification result acquisition request sent by the first institution by initiating a first transaction, wherein the first transaction is used to invoke a first

smart contract deployed on the privacy computing unit.

14. The method according to claim 13, wherein the sending the user verification result acquisition request to the second institution specifically comprises:

invoking the first smart contract to send the user verification result acquisition request digitally signed by the privacy computing unit to the second institution; or

invoking the first smart contract to send the user verification result acquisition request digitally signed by the first smart contract to the second institution.

15. The method according to claim 11, wherein the receiving first encrypted data of a user corresponding to the user identity information and sent by the second institution, and decrypting the first encrypted data to obtain the first data of the user specifically comprises:

receiving a second transaction initiated by the second institution and used to invoke a second smart contract deployed on the privacy computing unit, wherein parameters in the second transaction comprise the user identity information and the first encrypted data of the user corresponding to the user identity information; and

decrypting the first encrypted data to obtain the first data of the user.

16. The method according to claim 11, wherein the obtaining second encrypted data of the user corresponding to the user identity information from the third institution, and decrypting the second encrypted data to obtain the second data of the user specifically comprises:

receiving a third transaction initiated by the third institution and used to invoke a third smart contract deployed on the privacy computing unit, wherein parameters in the third transaction comprise the second encrypted data of the user corresponding to the user identity information; and

decrypting the second encrypted data to obtain the second data of the user.

17. The method according to claim 11, wherein the performing matching verification on the first data and the second data specifically comprises:

invoking a fourth smart contract deployed on the privacy computing unit to perform matching verification on the first data and the second data.

18. The method according to claim 11, before the sending the user verification result acquisition request to the second institution, further comprising:

determining that the second institution is an institution satisfying a predetermined regulation.

19. The method according to claim 11, before the receiving first encrypted data of

~~a user corresponding to the user identity information and sent by the second institution, further comprising:~~

~~proving, by the privacy computing unit, an identity of the privacy computing unit to the second institution.~~

~~20. The method according to claim 11, before the obtaining second encrypted data of the user corresponding to the user identity information from the third institution, further comprising:~~

~~determining that the third institution is an institution satisfying a predetermined regulation.~~

~~21. The method according to claim 11, before the obtaining second encrypted data of the user corresponding to the user identity information from the third institution, further comprising:~~

~~proving, by the privacy computing unit, an identity of the privacy computing unit to the third institution.~~

~~22. The method according to claim 11, wherein the receiving first encrypted data of a user corresponding to the user identity information and sent by the second institution specifically comprises:~~

~~receiving the first encrypted data sent by the second institution and comprising a signature of the second institution.~~

~~23. The method according to claim 11, wherein the obtaining second encrypted data of the user corresponding to the user identity information from the third institution specifically comprises:~~

~~obtaining the second encrypted data comprising a signature of the third institution from the third institution.~~

~~24. The method according to claim 11, before the obtaining second encrypted data of the user corresponding to the user identity information from the third institution, further comprising:~~

~~sending a data acquisition request to the third institution, wherein the data acquisition request is used to request to obtain the user basic data of the user corresponding to the user identity information, and the data acquisition request comprises the identity information of the user.~~

~~25. The method according to claim 1 or 2, wherein the method further comprises:~~

~~sending a proof of the verification result to a blockchain.~~

~~26. The method according to claim 25, wherein the proof of the verification result~~

comprises: a verifiable claim signed by the privacy computing unit, or a hash value signed by the privacy computing unit, wherein the hash value is a hash value obtained by performing hash calculation on the verification result.

27. An information sharing apparatus, wherein the apparatus is applied to a privacy computing unit, and comprises:

an acquisition module, configured to obtain a user verification result acquisition request sent by a first institution;

a determining module, configured to determine a verification result of a user that is requested by the user verification result acquisition request, wherein the verification result is a verification result obtained by performing matching verification on first data and second data; the first data is user basic data obtained by decrypting first encrypted data of the user that is sent by a second institution; the second data is user basic data obtained by decrypting second encrypted data of the user that is sent by a third institution; and the third institution is a trustworthy institution; and

a first sending module, configured to send the verification result to the first institution.

28. The apparatus according to claim 27, wherein the first institution is a financial institution, and the second institution is a sales agency.

29. The apparatus according to claim 27 or 28, wherein the user verification result acquisition request comprises user identity information of the user.

30. The apparatus according to claim 29, 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 user basic data of the user.

31. The apparatus according to claim 29, 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.

32. The apparatus according to claim 29, wherein the user identity information comprises:

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

33. The apparatus according to claim 32, wherein the user identity information comprises:

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

~~34. The apparatus according to claim 29, wherein the user identity information comprised in the user verification result acquisition request is encrypted.~~

~~35. The apparatus according to claim 29, wherein the user verification result acquisition request further comprises a signature of the first institution.~~

~~36. The apparatus according to claim 29, wherein the determining module comprises:~~

~~a verification result determining unit, configured to determine a verification result of a user corresponding to the user identity information from a pre-generated user verification result, wherein the verification result of the user is a user verification result obtained by performing matching verification on the first data and the second data in advance.~~

~~37. The apparatus according to claim 29, wherein the determining module comprises:~~

~~a first sending unit, configured to send the user verification result acquisition request to the second institution;~~

~~a receiving unit, configured to: receive first encrypted data of a user corresponding to the user identity information and sent by the second institution, and decrypt the first encrypted data to obtain the first data of the user;~~

~~an acquisition unit, configured to obtain second encrypted data of the user corresponding to the user identity information from the third institution, and decrypting the second encrypted data to obtain the second data of the user; and~~

~~a verification unit, configured to perform matching verification on the first data and the second data to obtain the verification result of the user.~~

~~38. The apparatus according to claim 37, wherein the first sending unit is specifically configured to:~~

~~send the user verification result acquisition request to the second institution by using the privacy computing unit deployed on a blockchain; or~~

~~send the user verification result acquisition request to the second institution by using the privacy computing unit deployed off a blockchain.~~

~~39. The apparatus according to claim 37, wherein the acquisition module is specifically configured to:~~

~~obtain a user verification result acquisition request sent by the first institution by~~

initiating a first transaction, wherein the first transaction is used to invoke a first smart contract deployed on the privacy computing unit.

40. The apparatus according to claim 39, wherein the first sending unit is specifically configured to:

invoke the first smart contract to send the user verification result acquisition request digitally signed by the privacy computing unit to the second institution; or

invoke the first smart contract to send the user verification result acquisition request digitally signed by the first smart contract to the second institution.

41. The apparatus according to claim 37, wherein the receiving unit is specifically configured to:

receive a second transaction initiated by the second institution and used to invoke a second smart contract deployed on the privacy computing unit, wherein parameters in the second transaction comprise the user identity information and the first encrypted data of the user corresponding to the user identity information; and

decrypt the first encrypted data to obtain the first data of the user.

42. The apparatus according to claim 37, wherein the acquisition unit is specifically configured to:

receive a third transaction initiated by the third institution and used to invoke a third smart contract deployed on the privacy computing unit, wherein parameters in the third transaction comprise the second encrypted data of the user corresponding to the user identity information; and

decrypt the second encrypted data to obtain the second data of the user.

43. The apparatus according to claim 37, wherein the verification unit is specifically configured to:

invoke a fourth smart contract deployed on the privacy computing unit to perform matching verification on the first data and the second data.

44. The apparatus according to claim 37, wherein the determining module further comprises:

a first determining unit, configured to determine that the second institution is an institution satisfying a predetermined regulation.

45. The apparatus according to claim 37, wherein the determining module further comprises:

a first proving unit, configured to prove, by the privacy computing unit, an identity of the privacy computing unit to the second institution.

~~46. The apparatus according to claim 37, wherein the determining module further comprises:~~

~~a second determining unit, configured to determine that the third institution is an institution satisfying a predetermined regulation.~~

~~47. The apparatus according to claim 37, wherein the determining module further comprises:~~

~~a second proving unit, configured to prove, by the privacy computing unit, an identity of the privacy computing unit to the third institution.~~

~~48. The apparatus according to claim 37, wherein the receiving unit is specifically configured to:~~

~~receive the first encrypted data sent by the second institution and comprising a signature of the second institution.~~

~~49. The apparatus according to claim 37, wherein the acquisition unit is specifically configured to:~~

~~obtain the second encrypted data comprising a signature of the third institution from the third institution.~~

~~50. The apparatus according to claim 37, wherein the determining module further comprises:~~

~~a second sending unit, configured to send a data acquisition request to the third institution, wherein the data acquisition request is used to request to obtain the user basic data of the user corresponding to the user identity information, and the data acquisition request comprises the identity information of the user.~~

~~51. The apparatus according to claim 27 or 28, wherein the apparatus further comprises:~~

~~a second sending module, configured to send a proof of the verification result to a blockchain.~~

~~52. The apparatus according to claim 51, wherein the proof of the verification result comprises: a verifiable claim signed by the privacy computing unit, or a hash value signed by the privacy computing unit, wherein the hash value is a hash value obtained by performing hash calculation on the verification result.~~

~~53. An information sharing device, comprising:~~

~~at least one processor; and~~

~~a memory communicably coupled to the at least one processor; wherein~~

~~the memory stores instructions that can be executed by the at least one processor,~~

~~and the instructions are executed by the at least one processor, to enable the at least one processor to:~~

~~obtain a user verification result acquisition request sent by a first institution;~~

~~determine a verification result of a user that is requested by the user verification result acquisition request, wherein the verification result is a verification result obtained by performing matching verification on first data and second data; the first data is user basic data obtained by decrypting first encrypted data of the user that is sent by a second institution; the second data is user basic data obtained by decrypting second encrypted data of the user that is sent by a third institution; and the third institution is a trustworthy institution; and~~

~~send the verification result to the first institution~~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.