CLAIMS

What is claimed is:

1. A data verification method, wherein the method is applied to a privacy computing unit and comprises:

receiving a trigger instruction that is sent by a blockchain platform based on timed starting logic defined in a chain code;

performing verification processing on user basic data based on the trigger instruction to obtain a verification result, wherein the user basic data is obtained after first encrypted data sent by a first institution is decrypted, and the user basic data is user basic data obtained based on a user ID comprised in a data sharing request sent by a second institution, wherein the first institution and the second institution are different institutions; and

sending the verification result to the second institution.

2. The method according to claim 1, wherein the privacy computing unit is deployed on a node on the blockchain platform, or the privacy computing unit is deployed on a node off the blockchain platform.

3. The method according to claim 1, wherein the trigger instruction is sent by a node on the blockchain platform to the privacy computing unit on a node off the blockchain platform by using an oracle mechanism, and is used to start invoking a first smart contract deployed on the privacy computing unit.

4. The method according to claim 1, wherein the trigger instruction is used to start invoking a first smart contract deployed on the blockchain platform.

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

6. The method according to claim 1, wherein the user ID comprises:

an account registered by a user at the first institution; or

an account allocated to a user by a system of the first institution when the user initiates a purchase operation at the first institution.

7. The method according to claim 1, wherein the user ID comprises:

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

8. The method according to claim 7, wherein the digest value is obtained through hash calculation on one or more pieces of information of the user basic data and a salt value.

9. The method according to claim 1, before the performing verification processing on user basic data, further comprising:

obtaining, by using an oracle mechanism, the data sharing request sent by the second institution and comprising the user ID and the first encrypted data sent by the first institution, wherein the first encrypted data is encrypted user basic data corresponding to the user ID.

10. The method according to claim 1, before the performing verification processing on user basic data, further comprising:

obtaining the data sharing request sent by the second institution and comprising the user ID;

obtaining, based on the data sharing request, the first encrypted data sent by the first institution, wherein the first encrypted data is encrypted user basic data corresponding to the user ID; and

invoking a first smart contract to decrypt the first encrypted data.

11. The method according to claim 10, wherein the obtaining, based on the data sharing request, the first encrypted data sent by the first institution specifically comprises:

invoking a second smart contract, and sending the data sharing request to the first institution; and

obtaining the encrypted user basic data sent by the first institution and corresponding to the user ID.

12. The method according to claim 11, wherein before the obtaining the encrypted user basic data sent by the first institution and corresponding to the user ID, the method further comprises:

proving an identity of the privacy computing unit to the first institution.

13. The method according to claim 12, wherein the proving an identity of the privacy computing unit to the first institution specifically comprises:

sending a remote attestation report to the first institution, wherein the remote attestation report comprises self-recommendation information of the privacy computing unit about a trusted execution environment (TEE) and verification information of an authority organization for the self-recommendation information.

14. The method according to claim 11, wherein the invoking a second smart contract, and sending the data sharing request to the first institution specifically comprises:

invoking the second smart contract to send the data sharing request signed by using the privacy computing unit to the first institution; or

invoking the second smart contract to send the data sharing request signed by using the second smart contract to the first institution.

15. The method according to claim 1, wherein the user ID comprised in the data sharing request is sent by the first institution to the second institution.

16. The method according to claim 10, wherein the performing verification processing on user basic data specifically comprises:

invoking the first smart contract to perform verification processing on the user basic data.

17. The method according to claim 1, wherein the performing verification processing on user basic data specifically comprises:

obtaining second encrypted data sent by a trustworthy institution that stores trusted data corresponding to the user ID and obtained after the trusted data corresponding to the user ID is encrypted;

decrypting the second encrypted data by using a public key of the trustworthy institution to obtain the trusted data; and

verifying the user basic data based on the trusted data.

18. The method according to claim 16, wherein the method further comprises: sending a proof of the verification result to the blockchain platform.

19. The method according to claim 18, wherein the sending a proof of the verification result to the blockchain platform specifically comprises:

sending the proof of the verification result to the blockchain platform by using an oracle mechanism.

20. The method according to claim 18, wherein the proof of the verification result comprises a verifiable claim signed by the privacy computing unit or the first smart contract.

21. The method according to claim 20, wherein when verifying the verification result, a third institution verifies a signature of the verifiable claim by using a public key of the privacy computing unit or the first smart contract.

22. A method for starting a smart contract, wherein the method comprises:

running timed starting logic defined in a chain code;

determining, based on the timed starting logic, whether a current moment reaches a timed starting moment, to obtain a first determining result; and

if the first determining result is yes, sending an instruction used to start a first smart contract, wherein the first smart contract is used to perform verification processing on encrypted user basic data, and send a verification result to a specified address.

23. The method according to claim 22, wherein the sending an instruction used to start a first smart contract specifically comprises:

obtaining contract information of the first smart contract;

determining, based on the contract information, whether the first smart contract is an on-chain contract, to obtain a second determining result;

if the second determining result is yes, sending an instruction used to start the first smart contract deployed on a blockchain.

24. The method according to claim 23, wherein the method further comprises:

if the second determining result is no, sending an instruction for starting the first smart contract deployed on an off-chain node, wherein the instruction is used to invoke the first smart contract deployed on the off-chain node by using an oracle mechanism.

25. The method according to claim 22, wherein the determining whether a current moment reaches a timed starting moment specifically comprises:

monitoring in real time a new block generated on a blockchain;

obtaining timestamp information of the block after the block is detected;

determining the current moment based on the timestamp information; and

determining whether the current moment reaches the timed starting moment.

26. The method according to claim 24, wherein a verification result obtained after the off-chain node executes the first smart contract is fed back by the off-chain node to the blockchain by using the oracle mechanism.

27. A data verification apparatus, wherein the apparatus is applied to a privacy computing unit, and comprises:

a trigger instruction receiving module, configured to receive a trigger instruction that is sent by a blockchain platform based on timed starting logic defined in a chain code;

a data verification module, configured to perform verification processing on user basic data based on the trigger instruction to obtain a verification result, wherein the

user basic data is obtained after first encrypted data sent by a first institution is decrypted, and the user basic data is user basic data obtained based on a user ID comprised in a data sharing request sent by a second institution, wherein the first institution and the second institution are different institutions; and

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

28. The apparatus according to claim 27, wherein the privacy computing unit is deployed on a node on the blockchain platform, or the privacy computing unit is deployed on a node off the blockchain platform.

29. The apparatus according to claim 27, wherein the trigger instruction is sent by a node on the blockchain platform to the privacy computing unit on a node off the blockchain platform by using an oracle mechanism, and is used to start invoking a first smart contract deployed on the privacy computing unit.

30. The apparatus according to claim 27, wherein the trigger instruction is used to start invoking a first smart contract deployed on the blockchain platform.

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

32. The apparatus according to claim 27, wherein the user ID comprises:

an account registered by a user at the first institution; or

an account allocated to a user by a system of the first institution when the user initiates a purchase operation at the first institution.

33. The apparatus according to claim 27, wherein the user ID comprises:

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

34. The apparatus according to claim 33, wherein the digest value is obtained through hash calculation on one or more pieces of information of the user basic data and a salt value.

35. The apparatus according to claim 27, wherein the apparatus further comprises:

a data acquisition module, configured to obtain, by using an oracle mechanism, the data sharing request sent by the second institution and comprising the user ID and the first encrypted data sent by the first institution, wherein the first encrypted data is encrypted user basic data corresponding to the user ID.

36. The apparatus according to claim 27, wherein the apparatus further comprises:

a data sharing request acquisition module, configured to obtain the data sharing request sent by the second institution and comprising the user ID;

a first encrypted data acquisition module, configured to obtain, based on the data sharing request, the first encrypted data sent by the first institution, wherein the first encrypted data is encrypted user basic data corresponding to the user ID; and

a decryption module, configured to invoke a first smart contract to decrypt the first encrypted data.

37. The apparatus according to claim 36, wherein the first encrypted data acquisition module specifically comprises:

a data sharing request sending unit, configured to invoke a second smart contract, and send the data sharing request to the first institution; and

a user basic data acquisition unit, configured to obtain the encrypted user basic data sent by the first institution and corresponding to the user ID.

38. The apparatus according to claim 37, wherein the first encrypted data acquisition module further comprises:

an identity proving unit, configured to: before the encrypted user basic data sent by the first institution and corresponding to the user ID is obtained, prove an identity of the privacy computing unit to the first institution.

39. The apparatus according to claim 38, wherein the identity proving unit is specifically configured to send a remote attestation report to the first institution, wherein the remote attestation report comprises self-recommendation information of the privacy computing unit about a TEE and verification information of an authority organization for the self-recommendation information.

40. The apparatus according to claim 37, wherein the data sharing request sending unit is specifically configured to:

invoke the second smart contract to send the data sharing request signed by using the privacy computing unit to the first institution; or

invoke the second smart contract to send the data sharing request signed by using the second smart contract to the first institution.

41. The apparatus according to claim 27, wherein the user ID comprised in the data sharing request is sent by the first institution to the second institution.

42. The apparatus according to claim 36, wherein the data verification module is specifically configured to invoke the first smart contract to perform verification processing on the user basic data.

43. The apparatus according to claim 27, wherein the data verification module specifically comprises:

a second encrypted data acquisition unit, configured to obtain second encrypted data sent by a trustworthy institution that stores trusted data corresponding to the user ID and obtained after the trusted data corresponding to the user ID is encrypted;

a second encrypted data decryption unit, configured to decrypt the second encrypted data by using a public key of the trustworthy institution to obtain the trusted data; and

a verification unit, configured to verify the user basic data based on the trusted data.

44. The apparatus according to claim 42, wherein the apparatus further comprises:

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

45. The apparatus according to claim 44, wherein the verification result proof sending module is specifically configured to send the proof of the verification result to the blockchain platform by using an oracle mechanism.

46. The apparatus according to claim 44, wherein the proof of the verification result comprises a verifiable claim signed by the privacy computing unit or the first smart contract.

47. The apparatus according to claim 46, wherein when verifying the verification result, a third institution verifies a signature of the verifiable claim by using a public key of the privacy computing unit or the first smart contract.

48. An apparatus for starting a smart contract, wherein the apparatus comprises:

a code running module, configured to run timed starting logic defined in a chain code;

a result determining module, configured to determine, based on the timed starting logic, whether a current moment reaches a timed starting moment, to obtain a first determining result; and

an instruction sending module, configured to: if the first determining result is yes, send an instruction used to start a first smart contract, wherein the first smart contract is used to perform verification processing on encrypted user basic data, and send a verification result to a specified address.

49. The apparatus according to claim 48, wherein the instruction sending module specifically comprises:

a contract information acquisition unit, configured to obtain contract information of the first smart contract;

a result determining unit, configured to determine, based on the contract information, whether the first smart contract is an on-chain contract, to obtain a second determining result; and

a first instruction sending determining unit, configured to: if the second determining result is yes, send an instruction used to start the first smart contract deployed on a blockchain.

50. The apparatus according to claim 49, wherein the instruction sending module further comprises:

a second instruction sending unit, configured to: if the second determining result is no, send an instruction for starting the first smart contract deployed on an off-chain node, wherein the instruction is used to invoke the first smart contract deployed on the off-chain node by using an oracle mechanism.

51. The apparatus according to claim 48, wherein the determining whether a current moment reaches a timed starting moment specifically comprises:

monitoring in real time a new block generated on a blockchain;

obtaining timestamp information of the block after the block is detected;

determining the current moment based on the timestamp information; and

determining whether the current moment reaches the timed starting moment.

52. The apparatus according to claim 50, wherein a verification result obtained after the off-chain node executes the first smart contract is fed back by the off-chain node to the blockchain by using an oracle mechanism.

53. A data verification device, comprising:

at least one processor; and

a memory communicatively connected 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:

receive a trigger instruction that is sent by a blockchain platform based on timed starting logic defined in a chain code;

perform verification processing on user basic data based on the trigger instruction to obtain a verification result, wherein the user basic data is obtained after first encrypted data sent by a first institution is decrypted, and the user basic data is user

basic data obtained based on a user ID comprised in a data sharing request sent by a second institution, wherein the first institution and the second institution are different institutions; and

send the verification result to the second institution.

54. A device for starting a smart contract, comprising:

at least one processor; and

a memory communicatively connected 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:

run timed starting logic defined in a chain code;

determine, based on the timed starting logic, whether a current moment reaches a timed starting moment, to obtain a first determining result; and

if the first determining result is yes, send an instruction used to start a first smart contract, wherein the first smart contract is used to perform verification processing on encrypted user basic data, and send a verification result to a specified address.

55. A computer readable medium on which computer readable instructions are stored, wherein the computer readable instructions can be executed by a processor to implement the method according to any one of claims 1 to 26.