CLAIMS

What is claimed is:

1. An information sharing method, comprising:

sending, by a first institution, a first sharing request to a privacy computing unit in a method of initiating a transaction for invoking a contract, wherein the first sharing request comprises a user ID of a first user and corresponding first anti-money laundering (AML) risk information, and a signature of the first institution, and wherein the user ID of the first user and the first AML risk information are encrypted;

sending, by a second institution, a second sharing request to the privacy computing unit in a method of initiating a transaction for invoking a contract, wherein the second sharing request comprises a user ID of a second user and corresponding second AML risk information, and a signature of the second institution, and wherein the user ID of the second user and the second AML risk information are encrypted;

acknowledging, by the privacy computing unit, that the first sharing request and the second sharing request comprise AML risk information; acknowledging, by the privacy computing unit, that the AML risk information comprised in the first sharing request and the second sharing request satisfies a predefined rule; and, when the first sharing request and the second sharing request comprise AML risk information that satisfies the predefined rule, matching, by the privacy computing unit, the user ID of the first user against the user ID of the second user, and if they are consistent, combining the first AML risk information and the second AML risk information for the user ID, and sending, by the privacy computing unit, a proof of the combined first AML risk information and second AML risk information to a blockchain, wherein the proof comprises a verifiable claim signed by the privacy computing unit;

verifying, by a regulatory organization when verifying the combined first AML risk information and second AML risk information of the first institution or the second institution, a signature of the verifiable claim by using a public key of the privacy computing unit; and

sending, by the privacy computing unit, after verifying identities of the first institution and the second institution by using a decentralized identity service (DIS) and a blockchain, and after the signature of the verifiable claim is verified by using the

public key of the privacy computing unit, the combined first AML risk information and second AML risk information to the first institution and the second institution.

2. The method according to claim 1, wherein the user ID of the first user comprises:

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

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

the user ID of the second user comprises:

an account registered by the second user at the second institution; or

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

3. The method according to claim 2, wherein the user ID of the first user comprises:

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

the user ID of the second user comprises:

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

4. The method according to claim 3, wherein the user ID of the first user comprises:

a digest value obtained through salting hash calculation on one or more pieces of information of the first user; and

the user ID of the second user comprises:

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

5. The method according to claim 1, wherein the user ID of the first user and the user ID of the second user are encrypted.

6. The method according to claim 1, wherein the first AML risk information and the second AML risk information are encrypted.

7. The method according to claim 1, wherein the sending, by a first institution, a first sharing request to a privacy computing unit comprises:

sending, by the first institution, the first sharing request to the privacy computing unit in a method of initiating a transaction for invoking a contract; and

the sending, by a second institution, a second sharing request to the privacy computing unit comprises:

sending, by the second institution, the second sharing request to the privacy computing unit in a method of initiating a transaction for invoking a contract.

8. The method according to claim 1, wherein the privacy computing unit is a privacy computing unit deployed on a blockchain system or a privacy computing unit deployed on a device outside a blockchain system.

9. The method according to claim 1, wherein the first sharing request comprises a signature of the first institution; and the second sharing request comprises a signature of the second institution.

10. The method according to claim 1, wherein the privacy computing unit is deployed with a smart contract, used to: receive sharing requests sent by at least two institutions, in response to the sharing requests, match the user ID of the first user in the first sharing request sent by the first institution against the user ID of the second user in the second sharing request sent by the second institution, and if they are consistent, combine the first AML risk information in the first sharing request and the second AML risk information in the second sharing request for the user ID; and further used to send combined first AML risk information and second AML risk information to the first institution and the second institution.

11. The method according to claim 1, wherein before sending the combined first AML risk information and second AML risk information to the first institution and the second institution, the privacy computing unit further verifies an identity of the first institution and an identity of the second institution.

12. The method according to claim 1, wherein the method further comprises:

sending, by the privacy computing unit, a proof of the combined first AML risk information and second AML risk information to a blockchain.

13. The method according to claim 12, wherein the proof comprises a verifiable claim signed by the privacy computing unit.

14. The method according to claim 13, wherein when verifying the combined first AML risk information and second AML risk information of the first institution and the second institution, a regulatory organization further verifies a signature of the verifiable claim by using a public key of the privacy computing unit.

15. The method according to claim 1, wherein the first sharing request sent by the first institution further comprises a decentralized identifier (DID) of the first institution,

and the second sharing request sent by the second institution further comprises a DID of the second institution.

16. The method according to claim 15, wherein the sending, by the privacy computing unit, the combined first AML risk information and second AML risk information to the first institution and the second institution comprises:

sending, by the privacy computing unit, the combined first AML risk information and second AML risk information to the first institution and the second institution respectively based on the matched and consistent DID of the first institution and the DID of the second institution.

17. The method according to claim 1, before the matching, by the privacy computing unit, the user ID of the first user against the user ID of the second user, further comprising:

acknowledging that a corresponding sharing request comprises AML risk information.

18. The method according to claim 17, wherein the acknowledging that a corresponding sharing request comprises AML risk information further comprises:

acknowledging that existing AML risk information satisfies a predefined rule.

19. The method according to claim 17 or 18, wherein matching is not performed if no AML risk information is included or if the included AML risk information does not satisfy the predefined rule.

20. An information sharing system, comprising:

a first institution, configured to send a first sharing request to a privacy computing unit in a method of initiating a transaction for invoking a contract, wherein the first sharing request comprises a user ID of a first user and corresponding first AML risk information, and a signature of the first institution, and wherein the user ID of the first user and the first AML risk information are encrypted;

a second institution, configured to send a second sharing request to the privacy computing unit in a method of initiating a transaction for invoking a contract, wherein the second sharing request comprises a user ID of a second user and corresponding second AML risk information, and a signature of the second institution, and wherein the user ID of the second user and the second AML risk information are encrypted; and

the privacy computing unit, configured to: acknowledge that the first sharing request and the second sharing request comprise AML risk information; acknowledge that the AML risk information comprised in the first sharing request and the second sharing request satisfies a predefined rule; when the first sharing request and the second sharing request comprise AML risk information that satisfies the predefined rule, match the user ID of the first user against the user ID of the second user; and, if the user ID of the first user and the user ID of the second user are consistent, combine the first AML risk information and the second AML risk information for the ID, and send a proof of the combined first AML risk information and second AML risk information to a blockchain, wherein the proof comprises a verifiable claim signed by the privacy computing unit; wherein when verifying the combined first AML risk information and second AML risk information of the first institution or the second institution, a regulatory organization further verifies a signature of the verifiable claim by using a public key of the privacy computing unit; and send the combined first AML risk information and second AML risk information to the first institution and the second institution after identities of the first institution and the second institution are verified by using a decentralized identity service (DIS) and a blockchain, and after the signature of the verifiable claim is verified by using the public key of the privacy computing unit.

21. The system according to claim 20, wherein the user ID of the first user comprises:

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

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

the user ID of the second user comprises:

an account registered by the second user at the second institution; or

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

22. The system according to claim 20, wherein the user ID of the first user comprises:

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

the user ID of the second user comprises:

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

23. The system according to claim 22, wherein the user ID of the first user comprises:

a digest value obtained through salting hash calculation on one or more pieces of information of the first user; and

the user ID of the second user comprises:

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

24. The system according to claim 20, wherein the user ID of the first user and the user ID of the second user are encrypted.

25. The system according to claim 20, wherein the first AML risk information and the second AML risk information are encrypted.

26. The system according to claim 20, wherein the sending, by a first institution, a first sharing request to a privacy computing unit comprises:

sending, by the first institution, the first sharing request to the privacy computing unit in a method of initiating a transaction for invoking a contract; and

the sending, by a second institution, a second sharing request to the privacy computing unit comprises:

sending, by the second institution, the second sharing request to the privacy computing unit in a method of initiating a transaction for invoking a contract.

27. The system according to claim 20, wherein the privacy computing unit is a privacy computing unit deployed on a blockchain system or a privacy computing unit deployed on a device outside a blockchain system.

28. The system according to claim 20, wherein the first sharing request comprises a signature of the first institution; and the second sharing request comprises a signature of the second institution.

29. The system according to claim 20, wherein the privacy computing unit is deployed with a smart contract, used to: receive sharing requests sent by at least two institutions, in response to the sharing requests, match the user ID of the first user in the first sharing request sent by the first institution against the user ID of the second user in the second sharing request sent by the second institution, and if they are consistent, combine the first AML risk information in the first sharing request and the

second AML risk information in the second sharing request for the user ID; and further used to send combined first AML risk information and second AML risk information to the first institution and the second institution.

30. The system according to claim 20, wherein before sending the combined first AML risk information and second AML risk information to the first institution and the second institution, the privacy computing unit further verifies an identity of the first institution and an identity of the second institution.

31. The system according to claim 20, wherein the system further comprises:

the privacy computing unit sends a proof of the combined first AML risk information and second AML risk information to a blockchain.

32. The system according to claim 31, wherein the proof comprises a verifiable claim signed by the privacy computing unit.

33. The system according to claim 32, wherein when verifying the combined first AML risk information and second AML risk information of the first institution and the second institution, a regulatory organization further verifies a signature of the verifiable claim by using a public key of the privacy computing unit.

34. The system according to claim 20, wherein the first sharing request sent by the first institution further comprises a decentralized identifier (DID) of the first institution, and the second sharing request sent by the second institution further comprises a DID of the second institution.

35. The system according to claim 34, wherein the sending, by the privacy computing unit, the combined first AML risk information and second AML risk information to the first institution and the second institution comprises:

sending, by the privacy computing unit, the combined first AML risk information and second AML risk information to the first institution and the second institution respectively based on the matched and consistent DID of the first institution and the DID of the second institution.

36. The system according to claim 20, before the matching, by the privacy computing unit, the user ID of the first user against the user ID of the second user, further comprising:

acknowledging that a corresponding sharing request comprises AML risk information.

37. The system according to claim 36, wherein the acknowledging that a corresponding sharing request comprises AML risk information further comprises:

acknowledging that existing AML risk information satisfies a predefined rule.

38. The system according to claim 36 or 37, wherein matching is not performed if no AML risk information is included or if the included AML risk information does not satisfy the predefined rule.