CLAIMS

What is claimed is:

1. An information sharing method, wherein the method is applied to a privacy computing unit comprising a trusted execution environment (TEE) deployed on a device outside a blockchain system and comprises:

obtaining a trigger instruction sent by an external server based on a timed triggering rule, wherein timed triggering logic is deployed on the external server;

in the TEE of the privacy computing unit, implementing a deployment operation on an off-chain smart contract;

in response to the trigger instruction, invoking, in the TEE of the privacy computing unit, the off-chain smart contract to combine first anti-money laundering (AML) risk information provided by a first institution and second AML risk information provided by a second institution to obtain combined third AML risk information, wherein the combined first AML risk information and second AML risk information correspond to the same encrypted user identifier;

sending the third AML risk information to the first institution;

generating a proof used to prove trustworthiness of the third AML risk information;

sending the proof to a blockchain system for storage;

wherein the proof comprises a verifiable claim signed by the privacy computing unit using a private key stored in the TEE of the privacy computing unit; and

wherein when verifying the third AML risk information of the first institution, a regulatory organization further verifies a signature of the verifiable claim by using a public key of the privacy computing unit corresponding to the private key stored in the TEE of the privacy computing unit.

2. The method according to claim 1, after the obtaining combined third AML risk information, further comprising:

sending the third AML risk information to the second institution.

3. The method according to claim 1, wherein the timed triggering rule comprises predetermined duration or a predetermined starting moment.

4. The method according to claim 1, wherein the first AML risk information and the second AML risk information are stored in a cloud storage server.

5. The method according to claim 1, wherein the provided AML risk information is encrypted.

6. The method according to claim 1, wherein the combining first AML risk information provided by a first institution and second AML risk information provided by a second institution specifically comprises:

obtaining a first user identifier corresponding to the first AML risk information;

obtaining a second user identifier corresponding to the second AML risk information; and

combining the first AML risk information and the second AML risk information that have the same user identifier, to obtain and store the combined third AML risk information.

7. The method according to claim 6, wherein the first AML risk information comprises a first risk label, and the second AML risk information comprises a second risk label; and

the combining the first AML risk information and the second AML risk information that have the same user identifier specifically comprises:

combining the first risk label and the second risk label to obtain a combined third risk label.

8. The method according to claim 6, after the obtaining and storing the combined third AML risk information, further comprising:

receiving a first sharing request sent by the first institution, wherein the first sharing request comprises a user identifier of a first user;

receiving a second sharing request sent by the second institution, wherein the second sharing request comprises a user identifier of a second user; and

matching the user identifier of the first user against the user identifier of the second user, and if they are consistent, sending the combined third AML risk information corresponding to the user identifier to the first institution and the second institution.

9. The method according to claim 8, wherein the first sharing request is sent by the first institution to the privacy computing unit by initiating a transaction for invoking a smart contract; and

the second sharing request is sent by the second institution to the privacy computing unit by initiating a transaction for invoking a smart contract.

10. The method according to claim 8, wherein the first sharing request comprises a signature of the first institution; and the second sharing request comprises a signature of the second institution.

11. The method according to claim 1, wherein the user identifier 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 an operation at the first institution.

12. The method according to claim 11, wherein the user identifier comprises:

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

13. The method according to claim 12, wherein the user identifier comprises:

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

14. The method according to claim 2, wherein before the sending the third AML risk information to the first institution, the method further comprises:

verifying an identity of the first institution; and

before the sending the third AML risk information to the second institution, the method further comprises:

verifying an identity of the second institution.

15. The method according to claim 1, before the combining first AML risk information provided by a first institution and second AML risk information provided by a second institution, further comprising:

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

16. The method according to claim 8, wherein the first sharing request further comprises a decentralized identifier (DID) of the first institution, and the second sharing request further comprises a DID of the second institution.

17. The method according to claim 16, wherein the sending the third AML risk information to the first institution specifically comprises:

sending the third AML risk information to the first institution based on the matched and consistent DID of the first institution.

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

receiving a third sharing request sent by a third institution, wherein the third sharing request comprises an identifier of the third institution;

determining whether the identifier of the third institution corresponds to the third AML risk information; and

sending the third AML risk information to the third institution if the identifier of the third institution corresponds to the third AML risk information.

19. The method according to claim 8, before the matching the user identifier of the first user against the user identifier of the second user, further comprising:

determining whether both the first sharing request and the second sharing request comprise AML risk information; and

performing no matching if any sharing request does not comprise AML risk information.

20. The method according to claim 19, after the determining whether both the first sharing request and the second sharing request comprise AML risk information, further comprising:

if both the first sharing request and the second sharing request comprise AML risk information, determining whether the AML risk information satisfies a predefined rule;

performing matching if the AML risk information satisfies the predefined rule; and

performing no matching if the AML risk information does not satisfy the predefined rule.

21. The method according to claim 20, wherein the predefined rule comprises: whether data corresponding to the risk information comprises a predefined risk label.

22. An information sharing triggering method, wherein the method comprises:

obtaining, by an external server, time information used to indicate a current moment, wherein timed triggering logic is deployed on the external server;

determining whether the time information satisfies a timed triggering rule in the timed triggering logic, to obtain a determining result; and

sending a trigger instruction to a privacy computing unit if the determining result indicates that the time information satisfies the timed triggering rule in the timed triggering logic, wherein the privacy computing unit comprises a trusted execution environment (TEE) deployed on a device outside a blockchain system, and wherein the trigger instruction is used to trigger the privacy computing unit to perform operations comprising: in the TEE of the privacy computing unit, implementing a deployment operation on an off-chain smart contract; in response to the trigger instruction, invoking, in the TEE of the privacy computing unit, the off-chain smart contract to combine first

anti-money laundering (AML) risk information provided by a first institution and second AML risk information provided by a second institution to obtain combined third AML risk information, wherein the combined first AML risk information and second AML risk information correspond to the same encrypted user identifier; and sending the third AML risk information to the first institution;

generating a proof used to prove trustworthiness of the third AML risk information; and sending the proof to a blockchain system for storage, wherein the proof comprises a verifiable claim signed by the privacy computing unit using a private key stored in the TEE of the privacy computing unit, and wherein when verifying the third AML risk information of the first institution, a regulatory organization further verifies a signature of the verifiable claim by using a public key of the privacy computing unit corresponding to the private key stored in the TEE of the privacy computing unit.

23. The method according to claim 22, wherein the timed triggering rule is triggered when timed duration reaches predetermined duration; or

the timed triggering rule is triggered when a current moment reaches a predetermined starting moment.

24. The method according to claim 22, after the determining whether the time information satisfies a timed triggering rule in the timed triggering logic, to obtain a determining result, further comprising:

if the determining result indicates that the time information does not satisfy the timed triggering rule in the timed triggering logic, obtaining a data amount of data to be verified stored in a cloud storage server;

determining whether the data amount reaches a predetermined data amount threshold; and

sending a trigger instruction to the privacy computing unit if the data amount reaches the predetermined data amount threshold.

25. An information sharing apparatus, wherein the apparatus is applied to a privacy computing unit comprising a trusted execution environment (TEE) deployed on a device outside a blockchain system, and the apparatus comprises:

a trigger instruction acquisition module, configured to obtain a trigger instruction sent by an external server based on a timed triggering rule, wherein timed triggering logic is deployed on the external server;

a risk information combination module, configured to: in the TEE of the privacy computing unit, implement a deployment operation on an off-chain smart contract, and

in response to the trigger instruction, invoke, in the TEE of the privacy computing unit, the off-chain smart contract to combine first anti-money laundering (AML) risk information provided by a first institution and second AML risk information provided by a second institution to obtain combined third AML risk information, wherein the combined first AML risk information and second AML risk information correspond to the same encrypted user identifier;

a combination result sending module, configured to send the third AML risk information to the first institution;

a proof generation module, configured to generate a proof used to prove trustworthiness of the third AML risk information, wherein the proof comprises a verifiable claim signed by the privacy computing unit using a private key stored in the TEE of the privacy computing unit; and

a proof sending module, configured to send the proof to a blockchain system for storage, wherein when verifying the third AML risk information of the first institution, a regulatory organization further verifies a signature of the verifiable claim by using a public key of the privacy computing unit corresponding to the private key stored in the TEE of the privacy computing unit.

26. An information sharing triggering apparatus, wherein the apparatus comprises:

a time information acquisition module, configured to obtain time information used to indicate a current moment for an external server, wherein timed triggering logic is deployed on the external server;

a first determining module, configured to determine whether the time information satisfies a timed triggering rule in the timed triggering logic, to obtain a determining result; and

a trigger instruction sending module, configured to send a trigger instruction to a privacy computing unit if the determining result indicates that the time information satisfies the timed triggering rule in the timed triggering logic, wherein the privacy computing unit comprises a trusted execution environment (TEE) deployed on a device outside a blockchain system, and wherein the trigger instruction is used to trigger the privacy computing unit to perform operations comprising: in the TEE of the privacy computing unit, implementing a deployment operation on an off-chain smart contract; in response to the trigger instruction, invoking, in the TEE of the privacy computing unit, the off-chain smart contract to combine first anti-money laundering (AML) risk information provided by a first institution and second AML risk information provided

by a second institution to obtain combined third AML risk information, wherein the combined first AML risk information and second AML risk information correspond to the same encrypted user identifier; sending the third AML risk information to the first institution; generating a proof used to prove trustworthiness of the third AML risk information; and sending the proof to a blockchain system for storage, wherein the proof comprises a verifiable claim signed by the privacy computing unit using a private key stored in the TEE of the privacy computing unit, and wherein when verifying the third AML risk information of the first institution, a regulatory organization further verifies a signature of the verifiable claim by using a public key of the privacy computing unit corresponding to the private key stored in the TEE of the privacy computing unit.

27. An information sharing device, applied to a privacy computing unit deployed on a device outside a blockchain system, comprising:

at least one processor, wherein the at least one processor comprises a trusted execution environment (TEE); 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:

obtain a trigger instruction sent by an external server based on a timed triggering rule, wherein timed triggering logic is deployed on the external server;

in the TEE, implement a deployment operation on an off-chain smart contract;

in response to the trigger instruction, invoke, in the TEE, the off-chain smart contract to combine first anti-money laundering (AML) risk information provided by a first institution and second AML risk information provided by a second institution to obtain combined third AML risk information, wherein the combined first AML risk information and second AML risk information correspond to the same encrypted user identifier; and

send the third AML risk information to the first institution;

generate a proof used to prove trustworthiness of the third AML risk information; and send the proof to a blockchain system for storage, wherein the proof comprises a verifiable claim signed by the privacy computing unit using a private key stored in the TEE, and wherein when verifying the third AML risk information of the first institution, a regulatory organization further verifies a signature of the verifiable claim by using a

public key of the privacy computing unit corresponding to the private key stored in the TEE.

28. An information sharing triggering 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:

obtain time information used to indicate a current moment for an external server, wherein timed triggering logic is deployed on the external server;

determine whether the time information satisfies a timed triggering rule in the timed triggering logic, to obtain a determining result; and

send a trigger instruction to a privacy computing unit if the determining result indicates that the time information satisfies the timed triggering rule in the timed triggering logic, wherein the privacy computing unit comprises a trusted execution environment (TEE) deployed on a device outside a blockchain system, and wherein the trigger instruction is used to trigger the privacy computing unit to perform operations comprising: in the TEE of the privacy computing unit, implementing a deployment operation on an off-chain smart contract; in response to the trigger instruction, invoking, in the TEE of the privacy computing unit, the off-chain smart contract to combine first anti-money laundering (AML) risk information provided by a first institution and second AML risk information provided by a second institution to obtain combined third AML risk information, wherein the combined first AML risk information and second AML risk information correspond to the same encrypted user identifier; and

sending the third AML risk information to the first institution;

generating a proof used to prove trustworthiness of the third AML risk information; and sending the proof to a blockchain system for storage, wherein the proof comprises a verifiable claim signed by the privacy computing unit using a private key stored in the TEE of the privacy computing unit, and wherein when verifying the third AML risk information of the first institution, a regulatory organization further verifies a signature of the verifiable claim by using a public key of the privacy computing unit corresponding to the private key stored in the TEE of the privacy computing unit.