CLAIMS

What is claimed is:

1. A computer-implemented method, comprising:

receiving, from a blockchain network by a trusted execution environment (TEE) in a blockchain node, a trigger instruction based on a timed starting logic, wherein the timed starting logic identifies a starting time to execute a smart contract, wherein the timed starting logic is comprised in a chain code associated with the blockchain network, and wherein the chain code comprises information of a blockchain account and is executable by the blockchain node to determine the information of the blockchain account;

combining, by the TEE, first anti-money laundering (AML) risk information and second AML risk information based on the trigger instruction to obtain a combination result, wherein the first AML risk information is sent by a first institution for a first user ID of a user, the second AML risk information is sent by a second institution for the user; and

sending, by the TEE, the combination result to the first institution.

2. The computer-implemented method of claim 1, wherein the trigger instruction is sent by a node on the blockchain network to the TEE deployed on an off-chain node outside of the blockchain network, and wherein the trigger instruction triggers a first smart contract deployed in the TEE, and the first smart contract is configured to combine the first AML risk information and the second AML risk information.

3. The computer-implemented method of claim 1, wherein the first user ID comprises an account registered by the user at the first institution or assigned to the user by the first institution in response to an operation initiated by the user at the first institution.

4. The computer-implemented method of claim 1, wherein the TEE is deployed on a blockchain node of the blockchain network, and wherein the method comprises:

obtaining, from the first institution by the TEE, a first sharing request, wherein the first sharing request comprises the first user ID and the first AML risk information, and the first sharing request is stored in an off-chain node outside of the blockchain network; and

obtaining, from the second institution by the, a second sharing request, wherein the second sharing request comprises a second user ID and the second AML risk information, and the second sharing request is stored in the off-chain node.

5. The computer-implemented method of claim 1, wherein the TEE is deployed on a blockchain node of the blockchain network, and wherein the method comprises:

invoking, by the TEE, a second smart contract to obtain a first sharing request sent by the first institution and a second sharing request sent by the second institution, wherein the first sharing request comprises the first user ID and the first AML risk information, the second sharing request comprises a second user ID and the second AML risk information, and the first sharing request and the second sharing request are stored on the blockchain node.

6. The computer-implemented method of claim 1, wherein the first AML risk information comprises a first STR crime label, the second AML risk information comprises a second STR crime label, and the combination result is a result of combination of the first STR crime label and the second STR crime label.

7. The computer-implemented method of claim 4, further comprising proving an identity of the TEE to the first institution and 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, from a blockchain network by a trusted execution environment (TEE) in a blockchain node, a trigger instruction based on a timed starting logic, wherein the timed starting logic identifies a starting time to execute a smart contract, wherein the timed starting logic is comprised in a chain code associated with the blockchain network, and wherein the chain code comprises information of a blockchain account and is executable by the blockchain node to determine the information of the blockchain account;

combining, by the TEE, first anti-money laundering (AML) risk information and second AML risk information based on the trigger instruction to obtain a combination result, wherein the first AML risk information is sent by a first institution for a first user ID of a user, the second AML risk information is sent by a second institution for the user; and

sending, by the TEE, the combination result to the first institution.

9. The non-transitory, computer-readable medium of claim 8, wherein the trigger instruction is sent by a node on the blockchain network to the TEE deployed on an off-chain node outside of the blockchain network, and wherein the trigger instruction triggers a first smart

contract deployed in the TEE, and the first smart contract is configured to combine the first AML risk information and the second AML risk information.

10. The non-transitory, computer-readable medium of claim 8, wherein the first user ID comprises an account registered by the user at the first institution or assigned to the user by the first institution in response to an operation initiated by the user at the first institution.

11. The non-transitory, computer-readable medium of claim 8, wherein the TEE is deployed on a blockchain node of the blockchain network, and wherein the operations comprise:

obtaining, from the first institution by the TEE, a first sharing request, wherein the first sharing request comprises the first user ID and the first AML risk information, and the first sharing request is stored in an off-chain node outside of the blockchain network; and

obtaining, from the second institution by the, a second sharing request, wherein the second sharing request comprises a second user ID and the second AML risk information, and the second sharing request is stored in the off-chain node.

12. The non-transitory, computer-readable medium of claim 8, wherein the TEE is deployed on a blockchain node of the blockchain network, and wherein the operations comprise:

invoking, by the TEE, a second smart contract to obtain a first sharing request sent by the first institution and a second sharing request sent by the second institution, wherein the first sharing request comprises the first user ID and the first AML risk information, the second sharing request comprises a second user ID and the second AML risk information, and the first sharing request and the second sharing request are stored on the blockchain node.

13. The non-transitory, computer-readable medium of claim 8, wherein the first AML risk information comprises a first STR crime label, the second AML risk information comprises a second STR crime label, and the combination result is a result of combination of the first STR crime label and the second STR crime label.

14. The non-transitory, computer-readable medium of claim 11, wherein the operations further comprise proving an identity of the TEE to the first institution and 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, from a blockchain network by a trusted execution environment (TEE) in a blockchain node, a trigger instruction based on a timed starting logic, wherein the timed starting logic identifies a starting time to execute a smart contract, wherein the timed starting logic is comprised in a chain code associated with the blockchain network, and wherein the chain code comprises information of a blockchain account and is executable by the blockchain node to determine the information of the blockchain account;

combining, by the TEE, first anti-money laundering (AML) risk information and second AML risk information based on the trigger instruction to obtain a combination result, wherein the first AML risk information is sent by a first institution for a first user ID of a user, the second AML risk information is sent by a second institution for the user; and

sending, by the TEE, the combination result to the first institution.

16. The computer-implemented system of claim 15, wherein the trigger instruction is sent by a node on the blockchain network to the TEE deployed on an off-chain node outside of the blockchain network, and wherein the trigger instruction triggers a first smart contract deployed in the TEE, and the first smart contract is configured to combine the first AML risk information and the second AML risk information.

17. The computer-implemented system of claim 15, wherein the first user ID comprises an account registered by the user at the first institution or assigned to the user by the first institution in response to an operation initiated by the user at the first institution.

18. The computer-implemented system of claim 15, wherein the TEE is deployed on a blockchain node of the blockchain network, and wherein the operations comprise:

obtaining, from the first institution by the TEE, a first sharing request, wherein the first sharing request comprises the first user ID and the first AML risk information, and the first sharing request is stored in an off-chain node outside of the blockchain network; and

obtaining, from the second institution by the, a second sharing request, wherein the second sharing request comprises a second user ID and the second AML risk information, and the second sharing request is stored in the off-chain node.

19. The computer-implemented system of claim 15, wherein the TEE is deployed on a blockchain node of the blockchain network, and wherein the operations comprise:

invoking, by the TEE, a second smart contract to obtain a first sharing request sent by the first institution and a second sharing request sent by the second institution, wherein the first sharing request comprises the first user ID and the first AML risk information, the second sharing request comprises a second user ID and the second AML risk information, and the first sharing request and the second sharing request are stored on the blockchain node.

20. The computer-implemented system of claim 15, wherein the first AML risk information comprises a first STR crime label, the second AML risk information comprises a second STR crime label, and the combination result is a result of combination of the first STR crime label and the second STR crime label.