CLAIMS

What is claimed is:

1. A computer-implemented cross-chain attestation method, comprising:

transmitting, by a trusted execution environment (TEE) application, to a first blockchain, configuration information of a second blockchain, and remote attestation information of the configuration information, wherein the remote attestation information of the configuration information comprises proof that the configuration information is associated with the TEE application;

subsequent to transmitting the remote attestation information and the configuration information, receiving, by the TEE application, a cross-chain data request from a first blockchain node of the first blockchain;

after receiving the cross-chain data request, obtaining, by the TEE application, cross-chain data corresponding to the cross-chain data request from a second blockchain node of the second blockchain;

verifying, by the TEE application, the cross-chain data;

generating, by the TEE application, a signature using a private key of the TEE application, wherein a public key corresponding to the private key is stored in the first blockchain; and

returning, by the TEE application, the cross-chain data and the signature to the first blockchain node.

2. The computer-implemented method of claim 1, wherein the TEE application comprises a simple payment verification (SPV) node of the second blockchain, and wherein verifying the cross-chain data comprises:

verifying the cross-chain data based on header data of the second blockchain, wherein the header data is stored in the SPV node.

3. The computer-implemented method of claim 2, wherein the TEE application comprises a plurality of SPV nodes corresponding to different respective blockchains, including the SPV node of the second blockchain;

wherein the method further comprises selecting, by the TEE application, the SPV node of the second blockchain based on the cross-chain data request; and

wherein obtaining the cross-chain data comprises obtaining the cross-chain data using the SPV node.

4. The computer-implemented method of claim 1, comprising:

prior to receiving the cross-chain data request, transmitting, by the TEE application, to the first blockchain, the public key, a code measurement value, and initialization information of the TEE application.

5. The computer-implemented method of claim 1, wherein the TEE application operates as an enclave isolated from communication with another portion of a computing device in which the TEE application is located.

6. A non-transitory, computer-readable medium storing one or more instructions that, when executed by a computer system, cause the computer system to perform operations comprising:

transmitting, by a trusted execution environment (TEE) application, to a first blockchain, configuration information of a second blockchain, and remote attestation information of the configuration information, wherein the remote attestation information of the configuration information comprises proof that the configuration information is associated with the TEE application;

subsequent to transmitting the remote attestation information and the configuration information, receiving, by the TEE application, a cross-chain data request from a first blockchain node of the first blockchain;

after receiving the cross-chain data request, obtaining, by the TEE application, cross-chain data corresponding to the cross-chain data request from a second blockchain node of the second blockchain;

verifying, by the TEE application, the cross-chain data;

generating, by the TEE application, a signature using a private key of the TEE application, wherein a public key corresponding to the private key is stored in the first blockchain; and

returning, by the TEE application, the cross-chain data and the signature to the first blockchain node.

7. The non-transitory, computer-readable medium of claim 6, wherein the TEE

application comprises a simple payment verification (SPV) node of the second blockchain, and wherein verifying the cross-chain data comprises:

verifying the cross-chain data based on header data of the second blockchain, wherein the header data is stored in the SPV node.

8. The non-transitory, computer-readable medium of claim 7, wherein the TEE application comprises a plurality of SPV nodes corresponding to different respective blockchains, including the SPV node of the second blockchain;

wherein the operations further comprise selecting, by the TEE application, the SPV node of the second blockchain based on the cross-chain data request; and

wherein obtaining the cross-chain data comprises obtaining the cross-chain data using the SPV node.

9. The non-transitory, computer-readable medium of claim 6, wherein the operations comprise:

prior to receiving the cross-chain data request, transmitting, by the TEE application, to the first blockchain, the public key, a code measurement value, and data indicating one or more blockchains with which the TEE application is configured to communicate.

10. The non-transitory, computer-readable medium of claim 6, wherein the TEE application operates as an enclave isolated from communication with another portion of the computer system in which the TEE application is located.

11. 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, cause the one or more computers to perform one or more operations comprising:

transmitting, by a trusted execution environment (TEE) application, to a first blockchain, configuration information of a second blockchain, and remote attestation information of the configuration information,

wherein the remote attestation information of the configuration information

comprises proof that the configuration information is associated with the TEE application;

subsequent to transmitting the remote attestation information and the configuration information, receiving, by the TEE application, a cross-chain data request from a first blockchain node of the first blockchain;

after receiving the cross-chain data request, obtaining, by the TEE application, cross-chain data corresponding to the cross-chain data request from a second blockchain node of the second blockchain;

verifying, by the TEE application, the cross-chain data;

generating, by the TEE application, a signature using a private key of the TEE application, wherein a public key corresponding to the private key is stored in the first blockchain; and

returning, by the TEE application, the cross-chain data and the signature to the first blockchain node.

12. The computer-implemented system of claim 11, wherein the TEE application comprises a simple payment verification (SPV) node of the second blockchain, and wherein verifying the cross-chain data comprises:

verifying the cross-chain data based on header data of the second blockchain, wherein the header data is stored in the SPV node.

13. The computer-implemented system of claim 12, wherein the TEE application comprises a plurality of SPV nodes corresponding to different respective blockchains, including the SPV node of the second blockchain;

wherein the operations further comprise selecting, by the TEE application, the SPV node of the second blockchain based on the cross-chain data request; and

wherein obtaining the cross-chain data comprises obtaining the cross-chain data using the SPV node.

14. The computer-implemented system of claim 11, wherein the operations comprise:

prior to receiving the cross-chain data request, transmitting, by the TEE application, to the first blockchain, the public key, a code measurement value, and initialization information of the TEE application.

15. The computer-implemented system of claim 11, wherein the TEE application operates as an enclave isolated from communication with another portion of the computer-implemented system in which the TEE application is located.