

CLAIMS

What is claimed is:

1. A cross-chain data trusted management method, applied to a relay, wherein a
5 trusted execution environment (TEE) is loaded onto the relay to perform, in the TEE:

invoking, based on a cross-chain request from a first blockchain, cross-chain data
from a second blockchain that serves as a requested object, wherein the relay is
configured with a client device of the second blockchain;

loading a management rule set to manage the cross-chain data based on one or
10 more management rules comprised in the management rule set to obtain processed
data; and

returning, to the first blockchain, a response result that comprises an identity
signature of the relay, wherein the response result comprises the processed data.

15 2. The method according to claim 1, wherein the response result further
comprises information about the management rule set and a public key that uniquely
matches the information about the management rule set, to prove that the processed
data is obtained by managing the cross-chain data based on the one or more
management rules comprised in the management rule set.

20

3. The method according to claim 2, wherein the information about the
management rule set comprises a hash value formed, based on a preset algorithm,
from hash values that respectively correspond to the one or more management rules
comprised in the management rule set.

25

4. The method according to claim 3, wherein the preset algorithm is used to
organize the hash values that respectively correspond to the one or more management
rules comprised in the management rule set into a hash tree, wherein the information
about the management rule set comprises a root hash value of the hash tree.

30

5. The method according to claim 2, wherein the response result further
comprises a signature that is signed on the processed data by using a private key that

uniquely matches the information about the management rule set, and the signature is used to verify data integrity of the processed data.

6. A cross-chain data trusted management method, applied to a blockchain node of a first blockchain, wherein the method comprises:

creating a cross-chain request, wherein a requested object of the cross-chain request is a second blockchain, so that a relay invokes cross-chain data from the second blockchain by using a configured client device of the second blockchain, and wherein the relay is configured to manage the cross-chain data based on one or more management rules comprised in a management rule set to obtain processed data; and

obtaining a response result returned by the relay, wherein the response result is generated by the relay in a trusted execution environment (TEE), wherein the response result comprises the processed data, and wherein the response result comprises an identity signature of the relay.

7. The method according to claim 6, wherein the response result further comprises information about the management rule set and a public key that uniquely matches the management rule set, to indicate that the processed data is obtained by managing the cross-chain data based on the management rule set.

8. The method according to claim 7, further comprising:

initiating a verification request to the relay, wherein the verification request comprises the public key provided in the response result, and

wherein, when the relay returns information that is about the management rule set and that corresponds to the public key and the information is consistent with the information that is about the management rule set and that is comprised in the response result, it is determined that the public key comprised in the response result is from the relay and that the processed data is obtained by managing the cross-chain data based on the management rule set.

9. The method according to claim 7, wherein the response result further comprises a signature that is signed on the processed data by using a private key that uniquely matches the management rule set, and wherein the method comprises:

verifying the signature by using the public key comprised in the response result to determine data integrity of the processed data comprised in the response result.

10. A cross-chain data trusted management apparatus, applied to a relay, wherein
5 a trusted execution environment (TEE) is loaded onto the relay to implement units in the TEE, comprising:

an invoking unit, configured to invoke, based on a cross-chain request from a first blockchain, cross-chain data from a second blockchain that serves as a requested object, wherein the relay is configured with a client device of the second
10 blockchain;

a management unit, configured to load a management rule set to manage the cross-chain data based on one or more management rules comprised in the management rule set to obtain processed data; and

a first returning unit, configured to return, to the first blockchain, a response
15 result that comprises an identity signature of the relay, wherein the response result comprises the processed data.

11. The apparatus according to claim 10, wherein the response result further comprises information about the management rule set and a public key that uniquely
20 matches the information about the management rule set, to prove that the processed data is obtained by managing the cross-chain data based on the management rule set.

12. The apparatus according to claim 11, wherein the information about the management rule set comprises a hash value formed, based on a preset algorithm,
25 from hash values that respectively correspond to the one or more management rules comprised in the management rule set.

13. The apparatus according to claim 12, wherein the preset algorithm is used to organize the hash values that respectively correspond to the one or more management
30 rules comprised in the management rule set into a hash tree, wherein the information about the management rule set comprises a root hash value of the hash tree.

14. The apparatus according to claim 11, wherein the response result further comprises a signature that is signed on the processed data by using a private key that

uniquely matches the information about the management rule set, and wherein the signature is used to verify data integrity of the processed data.

15. A cross-chain data trusted management apparatus, applied to a blockchain
5 node of a first blockchain, wherein the apparatus comprises:

a creation unit, configured to create a cross-chain request, wherein a
requested object of the cross-chain request is a second blockchain, so that a relay
invokes cross-chain data from the second blockchain by using a configured client
device of the second blockchain, and wherein the relay is configured to manage the
10 cross-chain data based on one or more management rules comprised in a management
rule set to obtain processed data; and

an acquisition unit, configured to obtain a response result returned by the
relay, wherein the response result is generated by the relay in a trusted execution
environment (TEE), wherein the response result comprises the processed data, and
15 wherein the response result comprises an identity signature of the relay.

16. The apparatus according to claim 15, wherein the response result further
comprises information about the management rule set and a public key that uniquely
matches the management rule set, to indicate that the processed data is obtained by
20 managing the cross-chain data based on the management rule set.

17. The apparatus according to claim 16, further comprising:

a first request unit, configured to initiate a verification request to the relay,
wherein the verification request comprises the public key provided in the response
25 result, and

wherein, when the relay returns information that is about the management rule
set and that corresponds to the public key and when the information is consistent with
the information that is about the management rule set and that is comprised in the
response result, it is determined that the public key comprised in the response result is
30 from the relay and that the processed data is obtained by managing the cross-chain
data based on the management rule set.

18. The apparatus according to claim 16, wherein the response result further comprises a signature that is signed on the processed data by using a private key that uniquely matches the management rule set, and the apparatus further comprises:

5 a verification unit, configured to verify the signature by using the public key comprised in the response result to determine data integrity of the processed data comprised in the response result.

19. An electronic device, comprising:

a processor; and

10 a memory configured to store a processor-executable instruction, wherein the processor runs the processor-executable instruction to implement the method according to any one of claims 1 to 5.

20. An electronic device, comprising:

15 a processor; and

a memory configured to store a processor-executable instruction, wherein the processor runs the processor-executable instruction to implement the method according to any one of claims 6 to 9.