

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~~

generating a first root hash value based on the one or more management rules, the
first root hash value uniquely corresponding to a root hash value-locking key pair, the
root hash value-locking key pair comprising a root hash value-locking private key and
15 a root hash value-locking public key; and

returning, to the first blockchain, a response result that comprises an identity
signature of the relay, wherein the response result further comprises the processed data,
the first root hash value, the root hash value-locking public key, and a digital signature
generated using the processed data and the root hash value-locking private key.

20

~~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
25 comprised in the management rule set.~~

~~32.~~ The method according to claim ~~21~~, wherein ~~the information about the
management rule set comprises a~~ the first root hash value is formed, based on a preset
algorithm, from hash values that respectively correspond to the one or more
30 management rules comprised in the management rule set.

43. The method according to claim 32, 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, and wherein the root hash value of the hash tree is the first root hash value.

~~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.~~

64. 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 further comprises an identity signature of the relay, a first root hash value, a root hash value-locking public key, and a digital signature generated using the processed data and the root hash value-locking private key, and wherein the first root hash value is generated based on the one or more management rules, the first root hash value uniquely corresponding to a root hash value-locking key pair, the root hash value-locking key pair comprising the root hash value-locking private key and the root hash value-locking public key.

~~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.~~

85. The method according to claim 74, further comprising:

initiating a verification request to the relay, wherein the verification request comprises the root hash value-locking 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 root hash value-locking 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 root hash value-locking 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.

10 ~~96.~~ The method according to claim ~~74~~, ~~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 digital signature by using the root hash value-locking public key comprised in the response result to determine data integrity of the processed data
15 comprised in the response result.

~~107.~~ A cross-chain data trusted management apparatus, applied to a relay, wherein a trusted execution environment (TEE) is loaded onto the relay to implement units in the TEE, comprising:

20 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 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
25 rule set to obtain processed data;

a generating unit, configured to generate a first root hash value based on the one or more management rules, the first root hash value uniquely corresponding to a root hash value-locking key pair, the root hash value-locking key pair comprising a root hash value-locking private key and a root hash value-locking public key; and

30 a first returning unit, configured to return, to the first blockchain, a response result that comprises an identity signature of the relay, wherein the response result further comprises the processed data, the first root hash value, the root hash value-locking public key, and a digital signature generated using the processed data and the root hash value-locking private key.

~~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 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.~~

~~128.~~ The apparatus according to claim ~~117~~, wherein ~~the information about the management rule set comprises a~~ the first root hash value is 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.

~~139.~~ The apparatus according to claim ~~128~~, 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, and wherein the root hash value of the hash tree is the first root hash value.

~~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.~~

~~1510.~~ A cross-chain data trusted management apparatus, applied to a blockchain 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 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 wherein the response result further comprises an identity signature of the relay, a first root hash

value, a root hash value-locking public key, and a digital signature generated using the processed data and the root hash value-locking private key, and wherein the first root hash value is generated based on the one or more management rules, the first root hash value uniquely corresponding to a root hash value-locking key pair, the root hash value-locking key pair comprising the root hash value-locking private key and the root hash value-locking public key.

~~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 managing the cross-chain data based on the management rule set.~~

~~17~~11. The apparatus according to claim ~~16~~10, further comprising:
a first request unit, configured to initiate a verification request to the relay, wherein the verification request comprises the root hash value-locking 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 root hash value-locking 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 root hash value-locking 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.

~~18~~12. The apparatus according to claim ~~16~~10, 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:

a verification unit, configured to verify the digital signature by using the root hash value-locking public key comprised in the response result to determine data integrity of the processed data comprised in the response result.

~~19~~13. An electronic device, comprising:
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 1 to 53.

5 2014. An electronic device, comprising:

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 64 to 96.

10