

CLAIMS

1. A computer-implemented method for cross-chain and cross-network data transmission, comprising:

obtaining, by a first blockchain node of a first blockchain network, first data, wherein the first blockchain network is associated with the Internet and the first data is to be recorded on a second blockchain associated with a second blockchain network associated with a private network;

encrypting, by the first blockchain node, the first data to generate cyphertext of the first data; and

sending, by the first blockchain node, the cyphertext to a gateway, wherein the gateway comprises a server and a network device, the server stores the cyphertext that is provided to a second blockchain node of the second blockchain network, the cyphertext is decrypted by the second blockchain node to generate second data to be stored in the second blockchain, and the network device interconnects the first blockchain network and the second blockchain network.

2. The computer-implemented method of claim 1, further comprising, before obtaining the first data:

obtaining, by the first blockchain node, a cross-chain message that comprises raw data;

verifying, by the first blockchain node, that the raw data is stored in a first blockchain; and

converting, by the first blockchain node and based on a conversion rule, the raw data to obtain the first data, wherein the conversion rule is determined based on an input rule of the second blockchain network.

3. The computer-implemented method of claim 2, wherein the input rule of the second blockchain network comprises at least one of:

a plurality of input parameters of an input to the second blockchain network;

a coding scheme corresponding to each input parameter of the plurality of input parameters; or

an order to arrange the plurality of input parameters in the input.

4. The computer-implemented method of any preceding claim, wherein the raw data is obtained by a third blockchain node from the first blockchain, and the cross-chain message is generated and sent by the third blockchain node.
5. The computer-implemented method of any preceding claim, further comprising:
 - generating, by the first blockchain node, a first hash value of the first data; and
 - sending, by the first blockchain node, the first hash value to the gateway, wherein the first hash value is obtained by the second blockchain node from the gateway, wherein a second hash value of the second data is generated to be compared with the first hash value, and wherein the second data is stored in the second blockchain, in response to determining that the first hash value matches the second hash value.
6. The computer-implemented method of any preceding claim, further comprising:
 - generating, by the first blockchain node, one or more zero-knowledge proofs associated with the first data; and
 - sending, by the first blockchain node, the one or more zero-knowledge proofs to the gateway, wherein the one or more zero-knowledge proofs are used to determine that the cyphertext is secure, wherein the cyphertext is stored in the server, in response to determining that the cyphertext is secure.
7. The computer-implemented method of claim 6, wherein determining that the cyphertext is secure comprises at least one of:
 - determining that data to be decrypted from the cyphertext does not comprise any key word defined in a restricted list maintained by the gateway;
 - determining that the data to be decrypted from the cyphertext satisfies an input rule of the second blockchain network;
 - determining that a file to be decrypted from the cyphertext has a file type acceptable to the second blockchain network; or

determining that data to be decrypted from the cyphertext does not comprise a malware or virus.

8. The computer-implemented method of any preceding claim, wherein a data notification is sent to the second blockchain node notifying the second blockchain node that the cyphertext is stored in the server, wherein a data retrieval request in response to the data notification is received from the second blockchain node, and wherein a network connection in response to the data retrieval request is established between the gateway and the second blockchain node.

9. The computer-implemented method of any preceding claim, further comprising:

obtaining, by the first blockchain node, additional cyphertext from the gateway, wherein the gateway receives the additional cyphertext from the second blockchain network;

decrypting, by the first blockchain node, the additional cyphertext to generate third data; and

storing, by the first blockchain node, the third data in the first blockchain.

10. The computer-implemented method of any preceding claim, wherein the first blockchain network is associated with a plurality of parties of a contract, wherein the private network is associated with a bank or a court.

11. A system for cross-chain and cross-network data transmission, comprising:

one or more processors; and

one or more computer-readable memories coupled to the one or more processors and having instructions stored thereon that are executable by the one or more processors to perform the method of any of claims 1 to 10.

12. An apparatus for cross-chain and cross-network data transmission, the apparatus comprising a plurality of modules for performing the method of any of claims 1 to 10.