CLAIMS

1. A computer-implemented method performed by a blockchain node of a blockchain network, comprising:

receiving, by a blockchain node of a first blockchain network, a cross-chain request for relaying a cyphertext of a digital document to a second blockchain network, wherein the cross-chain request is sent from a first computing device associated with a guarantor, the digital document specifies a guarantee from the guarantor and one or more predetermined conditions of executing the guarantee, and wherein the guarantee is made by the guarantor to a beneficiary, and the digital document specifies one or more predetermined conditions of executing the guarantee;

storing the cross-chain request and the cyphertext to a first blockchain associated with the first blockchain network based on performing a consensus algorithm;

receiving a message from a second computing device for relaying information between the first blockchain network and the second blockchain network, the message includes a confirmation that the guarantee is accepted by the beneficiary and stored on a second blockchain associated with the second blockchain network; and

updating a status of the guarantee to indicate that the guarantee has been voided on the first blockchain.

2.The method of claim 1, further comprising:

receiving, by the blockchain node, one or more zero-knowledge proofs (ZKPs) associated with the cyphertext of the digital document, wherein the one or more ZKPs are related to one or more values associated with the guarantee; and

verifying that the one or more ZKPs are correct before storing the cyphertext to the first blockchain associated with the first blockchain network.

3.The method of claim 1, wherein the second computing device is at least one of (i) a blockchain node of the first blockchain network and the second blockchain network, or (ii) a blockchain node of a third blockchain network.

4.The method of claim 1, wherein the second computing device is a trusted device that supports a trusted computing environment (TEE) or a secure multi-party computation.

5.The method of claim 1, wherein the updating the status of the guarantee is performed in response to receiving a request to void the guarantee from the first computing device.

6.The method of claim 1, wherein the guarantee is in the form of a standby letter of credit (SBLC).

7.The method of claim 6, wherein the guarantee specifies that the guarantor shall pay the beneficiary a predetermined amount when the one or more predetermined conditions of executing the guarantee are met.

8.The method of claim 7, wherein the guarantor is an offshore bank that serves the applicant, the representative of the beneficiary is an onshore bank that serves the beneficiary, and the predetermined amount is paid to the beneficiary through the onshore bank when the one or more predetermined conditions are met.

9.The method of any preceding claim, wherein the one or more predetermined conditions include one or more of default conditions, amendment conditions, cancelation conditions, effective date, and expiration date.

10.The method of any previous claim, wherein the one or more ZKPs includes one or more of a range proof and a zero test, and at least one of the one or more ZKPs is generated based on homomorphic encryption.

11.The method of any previous claim, wherein the cyphertext is encrypted using an encryption key derived based on a linear secret sharing scheme.

12. A system for processing blockchain-based guarantee information, 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 11.

13. An apparatus for processing blockchain-based guarantee information, the apparatus comprising a plurality of modules for performing the method of any of claims 1 to 11.