CLAIMS

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

receiving a first cyphertext of a first digital document specifying a guarantee from a first computing device associated with at least a first guarantor and one or more zero-knowledge proofs (ZKPs) related to one or more values associated with the guarantee, wherein the guarantee is in a form of a standby letter of credit (SBLC), the guarantee specifies that the at least a first guarantor shall pay a beneficiary a predetermined amount when one or more predetermined conditions of executing the guarantee are met, and a request to modify the guarantee is a request to modify the predetermined amount to a reduced amount that equals to the predetermined amount less a payment amount already paid to the beneficiary, and a modified version of the first digital document includes the reduced amount, wherein the guarantee is made by the at least a first guarantor to the beneficiary, and the first digital document specifies the one or more predetermined conditions of executing the guarantee;

verifying that the one or more ZKPs are correct;

upon verifying that the one or more ZKPs are correct, storing the first cyphertext to a blockchain based on performing a consensus algorithm;

receiving a first message from a second computing device associated with the beneficiary or a representative of the beneficiary, the first message including the request to modify the guarantee;

sending a second message about the request to modify the guarantee to the first computing device; and

receiving from the first computing device a second cyphertext of the modified version of the first digital document specifying the guarantee.

2.The method of claim 1, further comprising:

storing the second cyphertext to the blockchain based on performing the consensus algorithm;

receiving a third message from the second computing device indicating an acceptance of the guarantee specified in the modified version of the first digital document; and

modifying the second cyphertext to update a status of the guarantee to indicate that the guarantee has been accepted by the beneficiary.

3. The method of claim 1, wherein the first message further includes a ZKP associated with the reduced amount, and the storing the second cyphertext is performed in response to successfully verifying the ZKP included in the first message.

4. The method of any previous claim, wherein the first guarantor is an offshore bank that serves an applicant of the first digital document, and the predetermined amount is paid to the beneficiary through an onshore bank that serves the beneficiary when the one or more predetermined conditions are met.

5. 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.

6. The method of any previous claim, wherein at least one of the one or more ZKPs is generated based on homomorphic encryption.

7. The method of any previous claim, wherein the one or more ZKPs includes one or more of a range proof and a zero test.

8. The method of any previous claim, wherein an encryption key for encrypting the first digital document is derived based on a linear secret sharing scheme.

9. The method of claim 1, wherein the guarantee is made by the first guarantor and a second guarantor to the beneficiary, and the guarantee specifies that the first guarantor and the

second guarantor shall pay the beneficiary the predetermined amount when the one or more predetermined conditions of executing the guarantee are met.

10. 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 9.

11. 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 9.