

## CLAIMS

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

receiving a cyphertext of a digital document specifying a guarantee and one or more zero-knowledge proofs (ZKPs) generated using a homomorphic encryption scheme for verifying values associated with the guarantee, wherein the guarantee is made by at least a first guarantor to a beneficiary, and the digital document specifies one or more predetermined conditions of executing the guarantee, wherein the one or more ZKPs comprise an encrypted actual loan amount, an encrypted remaining loanable amount, and an encrypted maximum loanable amount;

verifying the one or more ZKPs based on determining whether the encrypted actual loan amount and the encrypted remaining loanable amount add up to the encrypted maximum loanable amount;

upon successfully verifying the one or more ZKPs, storing the cyphertext to a blockchain based on performing a consensus algorithm;

receiving a drawdown request of the guarantee from a first computing device associated with the beneficiary or a representative of the beneficiary;

storing the drawdown request to the blockchain based on performing the consensus algorithm;

delivering a first message about the drawdown request to a second computing device associated with the first guarantor;

receiving a second message from the second computing device associated with the first guarantor indicating that the first guarantor agrees to make a payment to the beneficiary according to the guarantee;

updating a status of the guarantee stored in the blockchain to indicate that the drawdown request of the guarantee has been processed by the first guarantor;

delivering a third message to the first computing device associated with the beneficiary or the representative of the beneficiary indicating that the first guarantor agrees to make the payment to the beneficiary according to the guarantee;

receiving a fourth message from the first computing device associated with the beneficiary or the representative of the beneficiary indicating that the payment from the first guarantor has been received by the beneficiary; and

updating the status of the guarantee stored in the blockchain to indicate that the payment of the guarantee has been received by the beneficiary.

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

3.The method of claim 2, wherein the guarantee specifies that the first guarantor shall pay the beneficiary a predetermined amount when the one or more predetermined conditions of executing the guarantee are met.

4.The method of claim 3, wherein the first guarantor is an offshore bank that serves an applicant of the digital document, 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.

5.The method of claim 4, wherein the digital document further includes information that specifies an identity of the onshore bank.

6.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.

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 the cyphertext is encrypted using an encryption key 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, the guarantee is in a form of a standby letter of credit (SBLC), and the guarantee specifies that the first guarantor and the second guarantor shall pay the beneficiary a predetermined amount when the one or more predetermined conditions of executing the guarantee are met.

10.The method of any previous claim, wherein the consensus algorithm is based on one of proof of work (PoW), proof of stake (PoS), and practical Byzantine fault tolerance (PBFT).

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

receiving a cyphertext of a digital document specifying a guarantee and one or more zero-knowledge proofs (ZKPs) generated using a homomorphic encryption scheme for verifying values associated with the guarantee, wherein the guarantee is made by at least a first guarantor to a beneficiary, and the digital document specifies one or more predetermined conditions of executing the guarantee, wherein the one or more ZKPs comprise an encrypted actual loan amount, an encrypted remaining loanable amount, and an encrypted maximum loanable amount;

verifying the one or more ZKPs based on determining whether the encrypted actual loan amount and the encrypted remaining loanable amount add up to the encrypted maximum loanable amount;

upon successfully verifying the one or more ZKPs, storing the cyphertext to a blockchain based on performing a consensus algorithm;

receiving a drawdown request of the guarantee from a first computing device associated with the beneficiary or a representative of the beneficiary;

storing the drawdown request to the blockchain based on performing the consensus algorithm;

delivering a first message about the drawdown request to a second computing device associated with the first guarantor;

receiving a second message from the second computing device associated with the first guarantor, in which the second message includes a notice of dishonor indicating that the first guarantor does not agree to make payment to the beneficiary according to the guarantee;

storing the notice of dishonor in the blockchain based on performing the consensus algorithm;

delivering a third message to the first computing device associated with the beneficiary or the representative of the beneficiary indicating that the first guarantor, in which the third message includes the notice of dishonor;

receiving a fourth message from the first computing device associated with the beneficiary or the representative of the beneficiary indicating that the notice of dishonor has been received by the beneficiary or the representative of the beneficiary; and

updating a status of the guarantee stored in the blockchain to indicate that the drawdown request is closed.

12.The method of claim 11, wherein the guarantee is in a form of a standby letter of credit (SBLC).

13.The method of claim 12, wherein the guarantee specifies that the first guarantor shall pay the beneficiary a predetermined amount when the one or more predetermined conditions of executing the guarantee are met.

14.The method of claim 13, wherein the first guarantor is an offshore bank that serves an 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.

15.The method of claim 14, wherein the digital document further includes information that specifies an identity of the onshore bank.

16.The method of any of claims 11 to 15, wherein the one or more predetermined conditions include one or more of default conditions, amendment conditions, cancelation conditions, effective date, and expiration date.

17.The method of any claims 11 to 16, wherein the one or more ZKPs includes one or more of a range proof and a zero test.

18.The method of any of claims 11 to 17, wherein the cyphertext is encrypted using an encryption key derived based on a linear secret sharing scheme.

19.The method of claim 11, wherein the guarantee is made by the first guarantor and a second guarantor to the beneficiary, the guarantee is in a form of a standby letter of credit (SBLC), and the guarantee specifies that the first guarantor and the second guarantor shall pay the beneficiary a predetermined amount when the one or more predetermined conditions of executing the guarantee are met.

20.The method of any of claims 11 to 19, wherein the consensus algorithm is based on one of proof of work (PoW), proof of stake (PoS), and practical Byzantine fault tolerance (PBFT).

21. 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 20.

22. 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 20.