

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) related to one or more 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;

verifying the one or more ZKPs;

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

receiving a first message from a first computing device associated with the beneficiary or a representative of the beneficiary indicating there is no outstanding claim for the guarantee;

sending a second message to a second computing device associated with the first guarantor to confirm that the first guarantor is discharged from undertaking payment under the guarantee;

receiving a third message from the second computing device associated with the first guarantor requesting a status of the guarantee to be changed to expired; and

updating the status of the guarantee stored in the blockchain to indicate that the guarantee has expired.

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

3.The method of claim 2, wherein the guarantee specifies that the at least a 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 at least one of the one or more ZKPs is generated based on homomorphic encryption.

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

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

10.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 the 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.

11.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).

12.The method of any previous claim, comprising:

prior to receiving the first message, receiving a fourth message from the first computing device associated with the beneficiary or the representative of the beneficiary, in which the third message includes a request requesting a valid period of the guarantee to be extended; and

storing the request requesting the valid period of the guarantee to be extended in the blockchain.

13. 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 12.

14. 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 12.