

CLAIMS

1. A computer-implemented method performed by a computing system associated with at least one guarantor for processing guarantee information to be stored on a blockchain, the method comprising:

receiving, from a computing device associated with an applicant, an application of a guarantee made by at least a first guarantor to a beneficiary, wherein the application includes information associated with an identity of the applicant, an identity of the beneficiary, and one or more predetermined conditions of executing the guarantee;

generating a digital version of the guarantee based on the information included in the application;

encrypting the digital version to generate cyphertext of the guarantee;

generating one or more zero-knowledge proofs (ZKPs) related to one or more values associated with the guarantee; and

sending the cyphertext and the one or more ZKPs to a blockchain network to store the cyphertext on a blockchain, wherein the cyphertext is stored on the blockchain through consensus of blockchain nodes of the blockchain network after the one or more ZKPs are successfully verified by the blockchain nodes.

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 the applicant, 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 claim 4, wherein the application further includes information that specifies an identity of the onshore bank.

6.The method of any one of claims 2 to 5, wherein the application further includes information that proves the applicant is capable of paying off the predetermined amount in case of the applicant is in default of the SBLC.

7.The method of any preceding claim, wherein the identity of the applicant includes one or more of the applicant's name, address, phone number, e-mail address, and type of business.

8.The method of any preceding claim, wherein the identity of the beneficiary includes one or more of the beneficiary's name, address, phone number, e-mail address, and type of business.

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 at least one of the one or more ZKPs is generated based on homomorphic encryption.

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

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

13.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 and second 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 a first bank that serves the applicant, the second guarantor is a second bank that serves the applicant, and the application further includes information that proves the applicant has sufficient funds in the first and second banks to pay off the predetermined amount in case the applicant is in default of the SBLC.

15.The method of any previous claim, comprising, at a blockchain node of the blockchain network, verifying the one or more ZKPs and performing consensus based on the cyphertext of the guarantee after the one or more ZKPs are verified, and storing the cyphertext of the guarantee to the blockchain associated with the blockchain network after the consensus is successfully performed.

16.A computer-implemented method comprising:

receiving, at a first computing device, an application of a guarantee to be made by a guarantor to a beneficiary, wherein the application includes information associated with an identity of the applicant, an identity of the beneficiary, and one or more predetermined conditions of executing the guarantee;

transmitting the application to a second computing device associated with the guarantor;

receiving, at the first computing device, a digital version of the guarantee that is generated based on the application;

encrypting the digital version to generate a cyphertext of the guarantee;

generating one or more zero-knowledge proofs (ZKPs) related to one or more values associated with the guarantee; and

sending the cyphertext and the one or more ZKPs to a blockchain network to store the cyphertext on a blockchain, wherein the cyphertext is stored on the blockchain through consensus of blockchain nodes of the blockchain network after the one or more ZKPs are successfully verified by the blockchain nodes.

17.A system for implementing a trustable guarantee platform, the system comprising:

- a guarantee document encryption module;
- a zero knowledge proof generation module;
- a blockchain processing module;
- a guarantee issuance processing module configured to:

- receive an application for a guarantee from an applicant, wherein the guarantee document specifies a guarantee made by a first guarantor to a beneficiary, and the guarantee document specifies one or more predetermined conditions of executing the guarantee,

- identify a digital version of the guarantee,

- invoke the guarantee document encryption module to generate a cyphertext of the guarantee document,

- invoke the zero knowledge proof generation module to generate one or more zero-knowledge proofs (ZKPs) related to one or more values associated with the guarantee, and

- invoke the blockchain processing module to send the cyphertext and the one or more ZKPs to a blockchain network to store the cyphertext on a blockchain associated with the blockchain network, wherein the cyphertext is stored on the blockchain through consensus of blockchain nodes of the blockchain network after the one or more ZKPs are successfully verified by the blockchain nodes.

18. The system of claim 17, comprising a guarantee document generation module configured to generate the digital version of the guarantee document based on the information included in the application.

19. The system of claim 18, wherein the guarantee document generation module is configured to generate the guarantee document in a form of a standby letter of credit (SBLC) document.

20. The system of claim 18 or 19, wherein the guarantee document generation module is configured to generate the guarantee document to specify a predetermined amount that the first guarantor shall pay the beneficiary when the one or more predetermined conditions of executing the guarantee are met.

21. The system of claim 20, wherein the application for the guarantee includes information about an offshore bank that serves the applicant and information about an onshore bank that serves the beneficiary, in which the predetermined amount is paid to the beneficiary through the onshore bank when the one or more predetermined conditions are met, and

wherein the guarantee issuance processing module is configured to verify an identity of the offshore bank, and verify an identity of the onshore bank.

22. The system of any one of claims 19 to 21, wherein the application further includes information that proves the applicant is capable of paying off the predetermined amount in case the applicant is in default of the SBLC, and

wherein the guarantee issuance processing module is configured to verify that the applicant is capable of paying off the predetermined amount in case the applicant is in default of the SBLC based on the information provided in the application.

23. The system of any previous claim, wherein the one or more predetermined conditions include one or more of default conditions, amendment conditions, cancelation conditions, effective date, and expiration date.

24. The system of any previous claim, wherein the zero knowledge proof generation module is configured to generate at least one of the one or more ZKPs based on homomorphic encryption.

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

26. The system of any previous claim, wherein the guarantee document encryption module is configured to derive an encryption key for encrypting the digital version based on a linear secret sharing scheme.

27.The system of claim 17, wherein the guarantee issuance processing module is configured to process the application for the guarantee in which 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,

wherein the application includes information about the second guarantor, and the guarantee issuance processing module is configured to verify an identity of the second guarantor.

28.The system of claim 18, wherein the first guarantor is a first bank that serves the applicant, the second guarantor is a second bank that serves the applicant, and the application further includes information that proves the applicant has sufficient funds in the first bank and the second bank to pay off the predetermined amount in case the applicant is in default of the SBLC, and

wherein the guarantee issuance processing module is configured to verify, based on the information provided in the application, that the applicant has sufficient funds in the first bank and the second bank to pay off the predetermined amount in case the applicant is in default of the SBLC.

29.The system of any previous claim, wherein the blockchain processing module participates as one of several blockchain nodes of the blockchain network, and is configured to verify the one or more ZKPs and perform consensus based on the cyphertext of the guarantee after the one or more ZKPs are verified, and store the cyphertext of the guarantee to a local copy of the blockchain after the consensus is successfully performed.

30.The system of any previous claim, comprising a guarantee document revision module configured to facilitate revision of the guarantee document, wherein the guarantee document revision module is configured to invoke the blockchain processing module to send a revised guarantee document to the blockchain network to store the revised guarantee document on the blockchain.

31. The system of any previous claim, comprising a guarantee fulfillment processing module configured to facilitate a guarantee drawdown process.

32. The system of any previous claim, comprising a guarantee expiration processing module configured to facilitate a guarantee expiration process.

33. The system of any previous claim, comprising a guarantee cancellation processing module configured to facilitate a guarantee cancellation process.

34. The system of any previous claim, comprising a guarantee cross-chain processing module configured to handle processes that involve multiple blockchain networks.

35. An apparatus for processing guarantee information, the apparatus comprising a plurality of modules for performing the method of any of claims 1 to 16.