

What Is Claimed Is:

1. A computer-implemented method for providing privacy-preserving supply chain financing, the method comprising:

receiving a first transaction, the first transaction containing commitment values of a plurality of terms of a loan agreement;

determining whether the commitment values contained in the first transaction satisfy a set of requirements, the set of requirements comprising a set of equations the commitment values contained in the first transaction are required to satisfy;

in response to a determination that the commitment values contained in the first transaction satisfy the set of requirements, recording the first transaction on a blockchain;

receiving a second transaction, the second transaction indicating a disbursement of a loan made by a lender in accordance with the loan agreement; and

in response to receiving the second transaction, recording the second transaction on the blockchain and updating at least one commitment value of an account balance based on at least one of the commitment values contained in the first transaction.

2. The method of claim 1, further comprising:

receiving a third transaction, the third transaction indicating a payment made to the lender in accordance with the loan agreement; and

in response to receiving the third transaction, recording the third transaction on the blockchain and updating the at least one commitment value of the account balance based on at least one of the commitment values contained in the first transaction.

3. The method of any preceding claim, prior to receiving the first transaction, further comprising:

receiving a loan application submitted by a first user;

notifying a second user the receipt of the loan application submitted by the first user;

receiving, from the second user, a confirmation confirming a validity of information contained in the loan application;

in response to receiving the confirmation, notifying an administrator of the loan application;

receiving, from the administrator, an acceptance of the loan application; and

in response to receiving the acceptance of the loan application from the administrator, recording the loan application on the blockchain.

4. The method of claim 3, further comprising:

receiving a loan offer submitted by the lender in response to the loan application submitted by the first user;

notifying at least one of the first user and the second user the receipt of the loan offer; and

receiving the first transaction containing the commitment values of the plurality of terms of the loan agreement from at least one of the first user, the second user, and the lender.

5. The method of any preceding claim, wherein the method is performed by one or more nodes in a blockchain system implemented to operate the blockchain.

6. The method of any preceding claim, wherein the determining whether the commitment values contained in the first transaction satisfy the set of requirements further comprises:

determining whether at least one of the commitment values contained in the first transaction is calculated based on a positive or non-negative number.

7. The method of any preceding claim, wherein the determining whether the commitment values contained in the first transaction satisfy the set of requirements further comprises:

determining whether at least one of the commitment values represents a commitment value of a fixed number.

8. The method of any preceding claim, wherein the updating the at least one commitment value of the account balance further comprises:

calculating a new commitment value to reflect an increase or a decrease of the account balance.

9. The method of claim 8, wherein the calculation is performed directly on commitment values.

10. A device for providing privacy-preserving supply chain financing, 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 providing privacy-preserving supply chain financing, the
apparatus comprising a plurality of modules for performing the method of any of claims 1
to 9.
12. A non-transitory computer-readable medium having stored therein instructions
that, when executed by a processor of a device, cause the device to perform the method
of any of claims 1 to 9.