

What Is Claimed Is:

1. A computer-implemented method for mitigating invoice financing fraud, the method comprising:

receiving a first transaction from a first user, the first transaction comprising a first commitment of an invoice and a first proof for proving the first user is an issuer of the invoice, the first commitment being generated based on a first token corresponding to the first user;

verifying the first proof;

receiving a second transaction from a second user, the second transaction comprising the first token corresponding to the first user, a second commitment of the invoice, and a second proof for proving the second user has certified the invoice, the second commitment being generated based on a second token corresponding to the second user and a certifying document generated by the second user;

determining that the first token is valid and verifying the second proof;

receiving a third transaction from a third user, the third transaction comprising the second token corresponding to the second user and a third proof generated by the third user; and

determining that the second token is valid and verifying the third proof, to determine no invoice financing fraud.

2. The method of claim 1, wherein the method is performed by one or more nodes in a blockchain system.

3. The method of claim 2, wherein the second user has a trusted identity registered on the blockchain system, the method further comprising:

verifying the trusted identity of the second user based on a signature utilized by the second user to sign the second transaction.

4. The method of any preceding claim, further comprising one of:

reporting a detection of fraud in response to a determination that the first proof is unacceptable;

reporting the detection of fraud in response to a determination that the first token is invalid or the second proof is unacceptable; or

reporting the detection of fraud in response to a determination that the second token is invalid or the third proof is unacceptable.

5. The method of any preceding claim, further comprising:

recording the first commitment of the invoice in a first invoice pool in response to a determination that the first proof is acceptable; and

recording the second commitment of the invoice in a second invoice pool and invalidating the first token in response to a determination that the first token is valid and that the second proof is acceptable.

6. The method of any preceding claim, further comprising:

invalidating the second token and reporting that no fraud is detected in response to a determination that the second token is valid and that the third proof is acceptable.

7. The method of any preceding claim, wherein the first proof, the second proof, and the third proof are zero-knowledge proofs.
8. The method of any preceding claim, wherein the first user is an issuer of the invoice and the first proof is a proof generated by the first user to prove that the first user is the issuer of the invoice.
9. The method of any preceding claim, wherein the second user is a trusted user and the second proof is a proof generated by the second user to prove that the second user has certified the invoice.
10. The method of any preceding claim, wherein the third user is a fund provider having received a request to provide invoice financing to the first user and the third proof is a proof generated by the third user to prove that the third user has verified validity of the request to provide invoice financing to the first user.
11. The method of any preceding claim, wherein the first commitment is generated by the first user with a first random value and the second commitment is generated by the second user with a second random value to unlink the first commitment and the second commitment.
12. A computer-implemented method for mitigating invoice financing fraud, the method comprising:

receiving a first transaction from a first user, the first transaction comprising a first commitment of an invoice and a first proof for proving the first user is an issuer

of the invoice, the first commitment being generated based on a first token corresponding to the first user;

verifying the first proof;

receiving a second transaction from a second user, the second transaction comprising the first token corresponding to the first user, a second commitment of the invoice, and a second proof for proving the second user is a receiver of the invoice, the second commitment being generated based on a second token corresponding to the second user;

determining that the first token is valid and verifying the second proof;

receiving a third transaction from a third user, the third transaction comprising the second token corresponding to the second user, a third commitment of the invoice, and a third proof for proving the third user has reviewed and certified the invoice, the third commitment being generated based on a third token corresponding to the third user and a certifying document generated by the third user;

determining that the second token is valid and verifying the third proof;

receiving a fourth transaction from a fourth user, the fourth transaction comprising the third token corresponding to the third user and a fourth proof generated by the fourth user; and

determining that the third token is valid and verifying the fourth proof, to determine no invoice financing fraud.

13. The method of claim 12, wherein the method is performed by one or more nodes in a blockchain system, and the third user has a trusted identity registered on the blockchain system, the method further comprising:

verifying the trusted identity of the third user based on a signature utilized by the third user to sign the third transaction.

14. A device for mitigating invoice financing fraud, 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 13.

15. An apparatus for mitigating invoice financing fraud, the apparatus comprising a plurality of modules for performing the method of any of claims 1 to 13.

16. 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 13.