

METHODS AND DEVICES FOR MITIGATING INVOICE FINANCING FRAUD

TECHNICAL FIELD

[0001] The specification relates generally to computer technologies, and more particularly, to methods and devices for mitigating invoice financing fraud.

BACKGROUND

[0002] Invoice financing is a way for businesses to borrow money against accounts receivable, including, e.g., the amounts due from customers. Invoice financing helps businesses improve cash flow, pay employees and suppliers, and reinvest in operations and growth earlier than they could if they had to wait until their customers paid their balances in full.

[0003] One of the risks associated with invoice financing is fraud. For example, some businesses may commit fraud by unilaterally producing fake invoices and attempt to borrow money using such invoices. Some businesses may commit fraud by borrowing against the same invoice multiple times from multiple fund providers or financiers. Fraudulent activities as such are difficult to detect and mitigate.

SUMMARY

[0004] In one aspect, a computer-implemented method for mitigating invoice financing fraud includes: 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, the first token itself being excluded from the first transaction; verifying the first proof; receiving a second transaction from

a second user, the second transaction and the first transaction containing different payload so as to unlink the second transaction and the first transaction, 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 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.

[0005] In another aspect, a device for mitigating invoice financing fraud includes: 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: receive 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; verify the first proof; receive 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; determine that the first token is valid and verify the second proof; receive 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 determine that the second token is valid and verify the third proof, to determine no invoice financing fraud.

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, the first token itself being excluded from the first transaction;

verifying the first proof;

receiving a second transaction from a second user, the second transaction and the first transaction containing different payload so as to unlink the second transaction and the first transaction, 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 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 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.
4. 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.
5. 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.
6. The method of any preceding claim, wherein the first proof, the second proof, and the third proof are zero-knowledge proofs.

7. 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.
8. The method of any preceding claim, wherein the second user is a receiver of the invoice and the second proof is a proof generated by the second user to prove that the second user is the receiver of the invoice.
9. 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.
10. 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.
11. The method of any preceding claim, wherein the first commitment and the second commitment are generated based on a one-way function and information regarding the first user, the second user, and at least a portion of the invoice.

12. The method of any preceding claim, wherein whether the first token or the second token is valid is determined based on whether the first token or the second token is listed in a used token list.

13. 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 12.

14. An apparatus for mitigating invoice financing fraud, the apparatus comprising a plurality of modules for performing the method of any of claims 1 to 12.

15. 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 12.