

METHODS AND DEVICES FOR PROVIDING PRIVACY-PRESERVING PROOF OF ACCOUNTS RECEIVABLE

ABSTRACT

Disclosed herein are methods, devices, and apparatuses, including computer programs stored on computer-readable media, for providing privacy-preserving proof of accounts receivable. One of the methods includes: receiving a plurality of encrypted data entries from a plurality of users; recording the plurality of encrypted data entries on a blockchain; receiving an anonymity data set from a particular user, the anonymity data set comprising at least one encrypted data entry associated with the particular user and at least one encrypted data entry associated with another user of the plurality of users; receiving a commitment of a sum of an amount specified in the at least one encrypted data entry; and recording the anonymity data set and the commitment on the blockchain to facilitate a verification of a range proof generated by the particular user for proving that the sum is greater than or equal to a threshold.

FIG. 4