What Is Claimed Is:

1. A computer-implemented method for providing privacy-preserving proof of accounts receivable, the method comprising:

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 of the plurality of users, 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 associated with the particular user contained in the anonymity data set, the sum excluding an amount specified in the at least one encrypted data entry associated with the other user of the plurality of users; 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 without revealing the sum.

2. The method of claim 1, wherein the plurality of encrypted data entries comprise at least one encrypted purchase order submitted by a buyer or at least one encrypted invoice submitted by a seller.

3. The method of claim 2, wherein a public key of the buyer is updated when an encrypted data entry associated with the buyer is generated, and a public key of the seller is updated when an encrypted data entry associated with the seller is generated.

4. The method of claim 3, wherein each particular encrypted data entry of the plurality of encrypted data entries comprises: the buyer’s updated public key, the seller’s updated public key, a commitment of the amount specified in the particular encrypted data entry, and a settlement status.

5. The method of claim 4, wherein each encrypted data entry of the anonymity data set has an unsettled settlement status.

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

receiving a proof associated with each particular encrypted data entry of the plurality of encrypted data entries; and

recording each particular encrypted data entry on the blockchain if the proof associated with the particular encrypted data entry is acceptable.

7. The method of claim 6, wherein the proof is a zero-knowledge proof.

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

receiving a zero-knowledge proof for proving that the commitment received is of the sum of the amount specified in the at least one encrypted data entry associated with the particular user.

9. The method of any preceding claim, wherein the range proof generated by the particular user for proving that the sum is greater than or equal to the threshold is a zero-knowledge range proof.

10. A device for providing privacy-preserving proof of accounts receivable, 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 proof of accounts receivable, 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.