

WHAT IS CLAIMED IS:

1. A computer-implemented method performed by a consensus node of a blockchain network, comprising:

- 5 receiving, from a first account, a digitally signed copy of
a plurality of note identifiers (IDs) identifying a corresponding plurality of notes,
a commitment of a transaction amount of a transaction between the first account and a second account, wherein the transaction comprises a transfer of at
10 least a portion of the plurality of notes from the first account to the second account,
a commitment of a difference value representing the difference between the transaction amount and a total value of the plurality of notes,
a first random number used to generate the commitment of the transaction
15 amount, wherein the first random number is encrypted by a public key of the second account,
an encrypted value of the transaction amount, wherein the encrypted value of the transaction amount is encrypted by the public key of the second account,
an encrypted value of a second random number used to generate the
20 commitment of the difference value, wherein the encrypted value of the second random number is encrypted by a public key of the first account,
an encrypted value of the difference value, wherein the encrypted value of the difference value is encrypted by the public key of the first account,
one or more range proofs, and
25 a zero-knowledge proof generated based on one or more selected random numbers;
verifying a digital signature of the digitally signed copy using the public key of the first account;
determining that the one or more range proofs prove that the transaction amount
30 and the difference value are greater than, or equal to, zero;

determining that the total value of the plurality of notes equals the sum of the transaction amount and the difference value, by comparing a sum of commitments corresponding, respectively, to each of the plurality of notes, to a sum of the commitment of the difference value and the commitment of the transaction amount; and

5 updating lists of notes held by each of the first account and the second account based on the plurality of notes, the transaction amount, and the difference value.

2. The computer-implemented method of claim 1, wherein each of the plurality of notes include one or more of a note type, a commitment of a note value, the note value
10 encrypted by public-key encryption or integrated encryption, and a random number used to generate the commitment encrypted by the public-key encryption or the integrated encryption.

3. The computer-implemented method of claim 2, further comprising determining
15 that each of the plurality of notes has the same note type.

4. The computer-implemented method of claim 2, wherein the commitment of the transaction amount, the commitment of the difference value, and the commitment of the note value are generated using a commitment scheme that is homomorphic.
20

5. The computer-implemented method of claim 1, wherein updating the lists of notes comprises adding, to a list of the first account, an entry comprising the commitment of the difference value.

25 6. The computer-implemented method of claim 1, wherein each of the plurality of note IDs includes a transaction address and an index number indicating an order of the corresponding note in transaction output, and wherein the transaction address is generated by hashing transaction information of the transaction.

30 7. The computer-implemented method of claim 1, further comprising determining that each of the plurality of note IDs is associated with the first account.

8. The computer-implemented method of claim 1, wherein the first random number and the transaction amount are encrypted by a public key of the second account based on Paillier encryption or Okamoto-Uchiyama encryption.

5

9. The computer-implemented method of claim 1, comprising
determining that the transaction amount in the commitment of the transaction
amount is the same as the transaction amount that is encrypted, and
determining that a random number used to generate the commitment of the
transaction amount is the same as the first random number.

10

10. A non-transitory computer-readable storage medium coupled to one or more
processors and having instructions stored thereon which, when executed by the one or
more processors, cause the one or more processors to perform operations in accordance
with the method of one or more of claims 1-9.

15

11. A system, comprising:
a computing device; and
a computer-readable storage device coupled to the computing device and having
instructions stored thereon which, when executed by the computing device, cause the
computing device to perform operations in accordance with the method of one or more of
claims 1-9.

20