

CLAIMS

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

receiving, from a first account, a digitally signed copy of:

a plurality of note identifiers 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 least a portion of the corresponding plurality of notes from the first account to the second account;

a commitment of a difference value representing a difference between the transaction amount and a total value of the corresponding plurality of notes;

an encrypted value of a first random number used to generate the commitment of the difference value, wherein the encrypted value of the first random number is encrypted by a public key of the first account; ~~and~~

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; and

receiving a second random number used to generate the commitment of the transaction amount, wherein the second random number is encrypted by a public key of the second account;

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

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

~~2. The computer-implemented method of claim 1, comprising:~~

~~receiving a second random number used to generate the commitment of the transaction amount, wherein the second random number is encrypted by a public key of the second account.~~

23. The computer-implemented method of claim 12, comprising:

determining that a random number used to generate the commitment of the transaction amount is identical to the second random number.

34. The computer-implemented method of claim 1, comprising:
receiving an encrypted value of the transaction amount, wherein the encrypted value of the transaction amount is encrypted by a public key of the second account.

45. The computer-implemented method of claim 34, comprising:
determining that the transaction amount in the commitment of the transaction amount is identical to the transaction amount that is encrypted.

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

67. The computer-implemented method of claim 56, further comprising determining that each note of the corresponding plurality of notes has an identical note type.

78. 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.

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

~~910~~. The computer-implemented method of claim 1, further comprising determining that each note identifier of the plurality of note identifiers is associated with the first account.

~~101~~. 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 computer-implemented method of one or more of claims 1-~~910~~.

~~112~~. A computer-implemented 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 computer-implemented method of one or more of claims 1-~~910~~.