

WHAT IS CLAIMED IS:

1. A computer-implemented method for validating blockchain transactions based on account models, comprising:

5 receiving, by a consensus node of a blockchain network, transaction data and a digital signature of the transaction data, wherein the transaction data includes an encrypted transaction amount, a random number, and an unencrypted transaction amount to be transferred from either a public account of a first user node to a private account of a second user node, or from a private account of the first user node to a public account of
10 the second user node, wherein each public account comprises a balance and each private account comprises an encrypted balance, wherein the digital signature is generated by digitally signing the transaction data using a private key of the first user node, and wherein the encrypted transaction amount is generated based on the random number and the unencrypted transaction amount using a commitment scheme;

15 verifying the digital signature of the transaction data using a public key of the first user node;

generating a second encrypted transaction amount based on the random number and the unencrypted transaction amount using the commitment scheme;

20 determining that the second encrypted transaction amount equals the received encrypted transaction amount; and

determining that either the unencrypted transaction amount is less than or equal to a balance of the public account of the first user node before transfer when the transaction is from the public account of the first user node to the private account of the second user node, or that the unencrypted transaction amount is less than or equal to an unencrypted
25 value of an encrypted balance of the private account of the first user node before transfer when the transaction is from the private account of the first user node to the public account of the second user node;

30 either subtracting the unencrypted transaction amount from the balance of the public account of the first user node, and adding the received encrypted transaction amount to an encrypted balance of the private account of the second user node, when the

transaction is from the public account of the first user node to the private account of the second user node, or

subtracting the received encrypted transaction amount from an encrypted balance of the private account of the first user node, and adding the unencrypted transaction amount to a balance of the public account of the second user node, when the transaction is from the private account of the first user node to the public account of the second user node.

2. The computer-implemented method of claim 1, wherein the balance of the public account of the first user node or of the second user node is viewable by the consensus node, and wherein the unencrypted value of the encrypted balance of the private account of the first user node or of the second user node is viewable using a private key of the respective user node.

3. The computer-implemented method of claim 1, wherein the transaction is from the private account of the first user node to the public account of the second user node, and the method further comprises:

receiving, from the first user node, a range proof to prove that the unencrypted transaction amount is less than or equal to the unencrypted value of the encrypted balance of the private account of the first user node; and

wherein the transfer is determined valid, if the unencrypted transaction amount is less than or equal to the unencrypted value of the encrypted balance of the private account of the first user node based on the range proof.

4. The computer-implemented method of claim 1, wherein the first user node has both the public account of the first user node and the private account of the first user node, and

wherein a user associated with the first user node selects whether to perform the transaction using the public account of the first user node or the private account of the first user node.

5. The computer-implemented method of claim 1, wherein the commitment scheme is homomorphic.

6. 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 1-5.

7. 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 1-5.