

CLAIMS

1. A computer-implemented method performed by a consensus node for validating a transaction between a first node and a second node within a blockchain network, the method comprising:

receiving transaction data associated with the transaction, the transaction data comprising: data representative of a plurality of assets, a first commitment that hides a first random number and a transaction amount of the transaction, a second commitment that hides a second random number and a change calculated based on deducting the transaction amount from a total value of the plurality of assets, the transaction amount and a third random number both encrypted by a public key of the second node based on a probabilistic homomorphic encryption (HE) scheme, the change and a fourth random number both encrypted by a public key of the first node based on the probabilistic HE scheme, one or more range proofs, a zero-knowledge proof (ZKP), and a digital signature generated based on a private key corresponding to the public key of the first node;

verifying the digital signature based on the public key of the first node;

determining that the one or more range proofs prove that the transaction amount and the change are each greater than, or equal to, zero;

determining that the total value of the plurality of assets equals a sum of the transaction amount and the change; and

determining, based on the ZKP, that the transaction is valid by determining that the first random number is equal to the third random number, the second random number is equal to the fourth random number, and the transaction amount hidden in the first commitment is equal to the transaction amount encrypted by the public key of the second node.

2. The computer-implemented method of claim 1, wherein the transaction is performed between an account associated with the first node and an account associated with the second node, and the method further comprises updating, after determining that the transaction is valid, the account associated with the first node and the account associated with the second node based on the transaction amount and the change.

3. The computer-implemented method of claim 1, wherein each of the plurality of assets is associated with one or more of an asset type, an asset value hidden in a commitment, and a random number used for generating the commitment.

4. The computer-implemented method of claim 3, further comprising determining that each of the plurality of assets is associated with a same asset type.

5. The computer-implemented method of claim 3, wherein the first commitment, the second commitment, and the commitment that hides the asset value are generated based on a commitment scheme that is homomorphic, and wherein the determining that the total value of the plurality of assets equals the sum of the transaction amount and the change is performed based on homomorphism of the commitment scheme.

6. The computer-implemented method of claim 1, wherein the third random number is encrypted based on the probabilistic HE scheme by treating the transaction amount as a random number, and the fourth random number is encrypted based on the probabilistic HE scheme by treating the change as a random number.

7. The computer-implemented method of claim 1, wherein the first commitment and the second commitment are generated based on a Pedersen commitment scheme, and the probabilistic HE scheme is an Okamoto-Uchiyama (OU) encryption scheme.

8. The computer-implemented method of claim 7, wherein the ZKP comprises a Pedersen commitment that hides a fifth random number and a sixth random number, a cyphertext of the fifth random number and the sixth random number encrypted by the public key of the second account based on the OU encryption scheme, and a cyphertext of the fifth random number and the sixth random number encrypted by the public key of the first account based on the OU encryption scheme.

9. The computer-implemented method of claim 1, wherein the ZKP is generated and used for determining that the transaction is valid based on properties of the probabilistic HE scheme.

10. The computer-implemented method of claim 1, wherein the determining that the transaction is valid is performed based on the ZKP without interactions between the first node and the second node through outside of the blockchain network.

11. A non-transitory, computer-readable medium storing one or more instructions executable by a computer system to perform operations comprising:

receiving transaction data associated with a transaction between a first node and a second node within a blockchain network, the transaction data comprising: data representative of a plurality of assets, a first commitment that hides a first random number and a transaction amount of the transaction, a second commitment that hides a second random number and a change calculated based on deducting the transaction amount from a total value of the plurality of assets, the transaction amount and a third random number both encrypted by a public key of the second node based on a probabilistic homomorphic encryption (HE) scheme, the change and a fourth random number both encrypted by a public key of the first node based on the probabilistic HE scheme, one or more range proofs, a zero-knowledge proof (ZKP), and a digital signature generated based on a private key corresponding to the public key of the first node;

verifying the digital signature based on the public key of the first node;

determining that the one or more range proofs prove that the transaction amount and the change are each greater than, or equal to, zero;

determining that the total value of the plurality of assets equals a sum of the transaction amount and the change; and

determining, based on the ZKP, that the transaction is valid by determining that the first random number is equal to the third random number, the second random number is equal to the fourth random number, and the transaction amount hidden in the first commitment is equal to the transaction amount encrypted by the public key of the second node.

12. The non-transitory, computer-readable medium of claim 11, wherein the transaction is performed between an account associated with the first node and an account associated with the second node, and the method further comprises updating, after determining that the transaction is valid, the account associated with the first node and the account associated with the second node based on the transaction amount and the change.

13. The non-transitory, computer-readable medium of claim 11, wherein each of the plurality of assets is associated with one or more of an asset type, an asset value hidden in a commitment, and a random number used for generating the commitment.

14. The non-transitory, computer-readable medium of claim 13, wherein the operations further comprise determining that each of the plurality of assets is associated with a same asset type.

15. The non-transitory, computer-readable medium of claim 13, wherein the first commitment, the second commitment, and the commitment that hides the asset value are generated based on a commitment scheme that is homomorphic, and wherein the determining that the total value of the plurality of assets equals the sum of the transaction amount and the change is performed based on homomorphism of the commitment scheme.

16. The non-transitory, computer-readable medium of claim 11, wherein the third random number is encrypted based on the probabilistic HE scheme by treating the transaction amount as a random number, and the fourth random number is encrypted based on the probabilistic HE scheme by treating the change as a random number.

17. The non-transitory, computer-readable medium of claim 11, wherein the first commitment and the second commitment are generated based on a Pedersen commitment scheme, and the probabilistic HE scheme is an Okamoto-Uchiyama (OU) encryption scheme.

18. The non-transitory, computer-readable medium of claim 17, wherein the ZKP comprises a Pedersen commitment that hides a fifth random number and a sixth random number, a cyphertext of the fifth random number and the sixth random number encrypted by the public key of the second account based on the OU encryption scheme, and a cyphertext of the fifth random number and the sixth random number encrypted by the public key of the first account based on the OU encryption scheme.

19. The non-transitory, computer-readable medium of claim 11, wherein the ZKP is generated and used for determining that the transaction is valid based on properties of the probabilistic HE scheme.

20. The non-transitory, computer-readable medium of claim 11, wherein the determining that the transaction is valid is performed based on the ZKP without interactions between the first node and the second node through outside of the blockchain network.

21. A computer-implemented system, comprising:

one or more computers; and

one or more computer memory devices interoperably coupled with the one or more computers and having tangible, non-transitory, machine-readable media storing one or more instructions that, when executed by the one or more computers, perform one or more operations comprising:

receiving transaction data associated with a transaction between a first node and a second node within a blockchain network, the transaction data comprising: data representative of a plurality of assets, a first commitment that hides a first random number and a transaction amount of the transaction, a second commitment that hides a second random number and a change calculated based on deducting the transaction amount from a total value of the plurality of assets, the transaction amount and a third random number both encrypted by a public key of the second node based on a probabilistic homomorphic encryption (HE) scheme, the change and a fourth random number both encrypted by a public key of the first node based on the probabilistic HE scheme, one or more range proofs, a zero-

knowledge proof (ZKP), and a digital signature generated based on a private key corresponding to the public key of the first node;

verifying the digital signature based on the public key of the first node;

determining that the one or more range proofs prove that the transaction amount and the change are each greater than, or equal to, zero;

determining that the total value of the plurality of assets equals a sum of the transaction amount and the change; and

determining, based on the ZKP, that the transaction is valid by determining that the first random number is equal to the third random number, the second random number is equal to the fourth random number, and the transaction amount hidden in the first commitment is equal to the transaction amount encrypted by the public key of the second node.

22. The system of claim 21, wherein the transaction is performed between an account associated with the first node and an account associated with the second node, and the method further comprises updating, after determining that the transaction is valid, the account associated with the first node and the account associated with the second node based on the transaction amount and the change.

23. The system of claim 21, wherein each of the plurality of assets is associated with one or more of an asset type, an asset value hidden in a commitment, and a random number used for generating the commitment.

24. The system of claim 23, wherein the operations further comprise determining that each of the plurality of assets is associated with a same asset type.

25. The system of claim 23, wherein the first commitment, the second commitment, and the commitment that hides the asset value are generated based on a commitment scheme that is homomorphic, and wherein the determining that the total value of the plurality of assets equals the sum of the transaction amount and the change is performed based on homomorphism of the commitment scheme.

26. The system of claim 21, wherein the third random number is encrypted based on the probabilistic HE scheme by treating the transaction amount as a random number, and the fourth random number is encrypted based on the probabilistic HE scheme by treating the change as a random number.

27. The system of claim 21, wherein the first commitment and the second commitment are generated based on a Pedersen commitment scheme, and the probabilistic HE scheme is an Okamoto-Uchiyama (OU) encryption scheme.

28. The system of claim 27, wherein the ZKP comprises a Pedersen commitment that hides a fifth random number and a sixth random number, a cyphertext of the fifth random number and the sixth random number encrypted by the public key of the second account based on the OU encryption scheme, and a cyphertext of the fifth random number and the sixth random number encrypted by the public key of the first account based on the OU encryption scheme.

29. The system of claim 21, wherein the ZKP is generated and used for determining that the transaction is valid based on properties of the probabilistic HE scheme.

30. The system of claim 21, wherein the determining that the transaction is valid is performed based on the ZKP without interactions between the first node and the second node through outside of the blockchain network.