

CLAIMS

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 commitment value of a first amount of a balance transfer from a first account to a second account generated based on a first random number, wherein the first amount of the balance transfer and the first random number are encrypted using a first public key of the first account based on a probabilistic homomorphic encryption (HE) algorithm;

a second amount of the balance transfer and a second random number, wherein the second amount and the second random number are encrypted using a public key of the second account based on the probabilistic HE algorithm;

one or more range proofs; and

15 a set of values generated based on one or more selected random numbers;

verifying a digital signature corresponding to the digitally signed copy using a second public key of the first account corresponding to a private key used to generate the digital signature;

20 determining that the one or more range proofs prove that the amount of the balance transfer is greater than zero and less than or equal to a balance of the first account;

determining if the first amount and the second amount are the same and if the first random number and the second random number are the same based on the encrypted first and second amounts, the encrypted first and second random numbers, and the set of values; and

25 updating the balance of the first account and a balance of the second account based on the first amount of the balance transfer in response to determining the first amount and the second amount are the same and the first random number and the second random number are the same, wherein the selected random numbers are represented by r^* , t^* , $z1^*$, and $z2^*$; the selected random numbers are used to generate a , b , c , d , C , D , and E ; where $a = r^* + xr$, $b = t^* + xt$, $c = z1^* + xz1$, $d = z2^* + xz2$, $C = g^{r^*}h^{t^*}$, $D = u2^{r^*}v2^{z1^*}$, and $E = u2^{t^*}v2^{z2^*}$, where r is the first random number, t is the first amount of the balance transfer, $z1$ and $z2$ are random numbers used to

30

encrypt the second transaction amount and the second random number, x is a hash value generated based on hashing C, D, E, and g, and where h, u_2 , and v_2 are generators of an elliptical curve.

- 5 2. The computer-implemented method of claim 1, wherein the commitment value is generated using a commitment scheme that is homomorphic.
3. The computer-implemented method of claim 2, wherein the commitment scheme is a Pedersen commitment scheme.
- 10 4. The computer-implemented method of claim 1, wherein the probabilistic HE algorithm is an Okamoto-Uchiyama HE algorithm.
5. The computer-implemented method of claim 1, wherein the set of values is further
15 generated based on C, D, and E.
6. The computer-implemented method of claim 5 wherein the first amount and the second amount are the determined to be the same and the first random number and the second random number are determined to be the same based on properties of probabilistic HE.
- 20 7. The computer-implemented method of claim 6, wherein the first amount and the second amount are determined to be the same and the first random number and the second random number are determined to be the same if $g^a h^b = CT^x$, $u_2^a v_2^c = DZ_B1^x$, and $u_2^b v_2^d = EZ_B2^x$, where $T = g^r h^t$ is the commitment value of the amount of the balance transfer, $Z_B1 = u_2^r v_2^{z1}$,
25 $Z_B2 = u_2^t v_2^{z2}$.
8. The computer-implemented method of claim 1, wherein updating the balance of the first account and a balance of the second account is performed based on HE.
- 30 9. A non-transitory, computer-readable medium storing one or more instructions executable by a computer system to perform operations comprising:

receiving, from a first account:

a digitally signed copy of a commitment value of a first amount of a balance transfer from a first account to a second account generated based on a first random number, wherein the first amount of the balance transfer and the first random number are encrypted using a first public key of the first account based on a probabilistic homomorphic encryption (HE) algorithm;

a second amount of the balance transfer and a second random number, wherein the second amount and the second random number are encrypted using a public key of the second account based on the probabilistic HE algorithm;

one or more range proofs; and

a set of values generated based on one or more selected random numbers;

verifying a digital signature corresponding to the digitally signed copy using a second public key of the first account corresponding to a private key used to generate the digital signature;

determining that the one or more range proofs prove that the amount of the balance transfer is greater than zero and less than or equal to a balance of the first account;

determining if the first amount and the second amount are the same and if the first random number and the second random number are the same based on the encrypted first and second amounts, the encrypted first and second random numbers, and the set of values; and

updating the balance of the first account and a balance of the second account based on the first amount of the balance transfer in response to determining the first amount and the second amount are the same and the first random number and the second random number are the same, wherein the selected random numbers are represented by r^* , t^* , $z1^*$, and $z2^*$; the selected random numbers are used to generate a , b , c , d , C , D , and E ; where $a = r^* + xr$, $b = t^* + xt$, $c = z1^* + xz1$, $d = z2^* + xz2$, $C = g^{r^*}h^{t^*}$, $D = u2^{r^*}v2^{z1^*}$, and $E = u2^{t^*}v2^{z2^*}$, where r is the first random number, t is the first amount of the balance transfer, $z1$ and $z2$ are random numbers used to encrypt the second transaction amount and the second random number, x is a hash value generated based on hashing C , D , E , and g , and where h , $u2$, and $v2$ are generators of an elliptical curve.

10. The non-transitory, computer-readable medium of claim 9, wherein the commitment value is generated using a commitment scheme that is homomorphic.
11. The non-transitory, computer-readable medium of claim 10, wherein the commitment
5 scheme is a Pedersen commitment scheme.
12. The non-transitory, computer-readable medium of claim 9, wherein the probabilistic HE algorithm is an Okamoto-Uchiyama HE algorithm.
- 10 13. The non-transitory, computer-readable medium of claim 9, wherein the set of values is further generated based on C, D, and E.
14. The non-transitory, computer-readable medium of claim 13 wherein the first amount and the second amount are determined to be the same and the first random number and the
15 second random number are determined to be the same based on properties of probabilistic HE.
15. The non-transitory, computer-readable medium of claim 14, wherein the first amount and the second amount are determined to be the same and the first random number and the second random number are determined to be the same if $g^a h^b = CT^x$, $u2^a v2^c = DZ_B1^x$, and $u2^b v2^d =$
20 EZ_B2^x , where $T = g^r h^t$ is the commitment value of the amount of the balance transfer, $Z_B1 = u2^r v2^{z1}$, $Z_B2 = u2^t v2^{z2}$.
16. A system, comprising:
one or more computers; and
25 one or more computer-readable memories coupled to the one or more computers and having instructions stored thereon which are executable by the one or more computers to perform operations comprising:
receive, from a first account:
a digitally signed copy of a commitment value of a first amount of a balance
30 transfer from a first account to a second account generated based on a first random number, wherein the first amount of the balance transfer and the first random number are encrypted using

a first public key of the first account based on a probabilistic homomorphic encryption (HE) algorithm;

a second amount of the balance transfer and a second random number, wherein the second amount and the second random number are encrypted using a public key of the

5 second account based on the probabilistic HE algorithm;

one or more range proofs; and

a set of values generated based on one or more selected random numbers;

verify a digital signature corresponding to the digitally signed copy using a second public key of the first account corresponding to a private key used to generate the digital signature;

10 determine that the one or more range proofs prove that the amount of the balance transfer is greater than zero and less than or equal to a balance of the first account;

determine if the first amount and the second amount are the same and if the first random number and the second random number are the same based on the encrypted first and second amounts, the encrypted first and second random numbers, and the set of values; and

15 update the balance of the first account and a balance of the second account based on the first amount of the balance transfer in response to determining the first amount and the second amount are the same and the first random number and the second random number are the same, wherein the selected random numbers are represented by r^* , t^* , $z1^*$, and $z2^*$; the selected random numbers are used to generate a , b , c , d , C , D , and E ; where $a = r^* + xr$, $b = t^* + xt$, $c = z1^* + xz1$, $d = z2^* + xz2$, $C = g^{r^*}h^{t^*}$, $D = u2^{r^*}v2^{z1^*}$, and $E = u2^{t^*}v2^{z2^*}$, where r is the first random number, t is the first amount of the balance transfer, $z1$ and $z2$ are random numbers used to encrypt the second transaction amount and the second random number, x is a hash value generated based on hashing C , D , E , and g , and where h , $u2$, and $v2$ are generators of an elliptical curve.

25