WHAT IS CLAIMED IS:

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

receiving, from a first account associated with a blockchain node, a digitally signed copy of a commitment value of a transaction amount associated with a balance transfer from the first account to a second account generated based on a first random number, a second random number encrypted using a public key of the first account, a third random number encrypted using a public key of the second account, 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 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 transaction amount is greater than zero and less than, or equal to, a balance of the first account;

determining if the first random number, the second random number, and the third random number are the same based on the set of values; and

updating the balance of the first account and a balance of the second account based on the transaction amount of the balance transfer if the first random number, the second random number, and the third random number are the same,

wherein the second random number and the third random number are encrypted based on a deterministic homomorphic encryption (HE) scheme that has linear properties of $HE(a + b) = HE(a) * HE(b)$ and $HE(ab) = HE(b)^a$, where a and b are plaintext used for HE.

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.

4. The computer-implemented method of claim 1, wherein the selected random numbers are represented by *r1* and *t1*, and the selected random numbers are used to generate *r2* and *t2*, where $r2 = r1 + xr$, $t2 = t1 + xt$, where *r1* and *t1* represent the one or more selected random numbers, *r* is the first random number, *t* is the transaction amount of the balance transfer, *x* is a Hash value.

5. The computer-implemented method of claim 4, wherein the set of values is further generated based on T1, T1' and T1", where $T1 = g^{r1}h^{t1}$, T1' = HE_A(*r1*), T1" = HE_B(*r1*), where *g* and *h* are generators of an elliptical curve, and wherein HE_A(*r1*) is generated based on HE of *r1* using the public key of the first account and HE_B(*r1*) is generated based on HE of *r1* using the public key of the second account, and wherein *x* is generated based on hashing T1 , T1' and T1".

6. The computer-implemented method of claim 5, wherein the first random number, the second random number, and the third random number are determined to be the same based on properties of deterministic HE.

7. The computer-implemented method of claim 5, wherein the first random number, the second random number, and the third random number are determined to be the same if $g^{r2}h^{t2} = T^{x}T1$, HE_A(*r2*) = $T'^{x}T1'$, and HE_B(*r2*) = $T''^{x}T1''$, where $T = g^{r}h^{t}$, T' = HE_A(*r*), and T" = HE_B(*r*), and wherein HE_A(*r*) and HE_A(*r2*) are generated based on HE of *r* and *r2*, respectively, using the public key of the first account, HE_B(*r*) and HE_B(*r2*) are generated based on HE of *r* and *r2* using the public key of the second account.

8. The computer-implemented method of claim 1, wherein T, T', and T" form a ciphertext of the transaction amount *t*.

9. 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 homomorphic encryption.

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.

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.