CLAIMS

1. A computing system comprising:

at least one processor;

at least one memory communicatively coupled to the at least one processor; and

at least one network interface communicatively coupled to the at least one processor and configured to receive a master public key from a trusted third party device and a first public transaction key from a customer device;

wherein the at least one processor is configured to:

derive a second public transaction key from a second public account key;

derive a third public account key from the master public key;

derive a third public transaction key from the third public account key;

derive, using a hashing function, a multi-approval transaction address in a customer wallet from the first public transaction key derived from a first public account key, the second public transaction key, and the third public transaction key; and

wherein the at least one network interface is configured to transmit the multi-approval transaction address to the customer device.

2. The computing system of claim 1, wherein the first public transaction key, the second public transaction key, and the third public transaction key are non-extended keys.

3. The computing system of claim 1, wherein the customer device requires private keys corresponding to at least two of the first public transaction key, the second public transaction key, and the third public transaction key in order to transact from the multi-approval transaction address.

4. The computing system of claim 3, wherein the at least one network interface is configured to:

communicate a private key associated with the second public transaction key to the customer device.

5. The computing system of claim 1, wherein the at least one processor is configured to verify identity data from the customer device at least in part by:

comparing the identity data with stored identity data for a customer.

6. The computing system of claim 5, wherein the identity data comprises biometric data.

7. The computing system of claim 1, wherein the at least one network interface receives the master public key from at least one of a credit union or a bank acting as the trusted third party device.

8. The computing system of claim 1, wherein the customer wallet stores at least one of a security, a currency, a commodity, a bond, a fund, or a combination thereof.

9. The computing system of claim 1, wherein the at least one processor is further configured to:

determine the first public transaction key that was derived from the first public account key;

determine the second public transaction key that was derived from the second public account key; and

determine the third public transaction key that was derived from the third public account key.

10. The computing system of claim 1, wherein the customer device further:

produces a signed transaction by signing a transaction that transacts from the multi-approval transaction address to multiple output addresses, wherein the customer device signs the transaction using respective private keys associated with at least two of:

the first public transaction key;

the second public transaction key; and

the third public transaction key; and

sends the signed transaction across a network for recording on a distributed ledger.

11. A computerized method performed by at least a computing device, comprising:

receiving a first public transaction key at the computing device;

deriving a second public transaction key from a second public account key;

receiving a master public key at the computing device;

deriving a third public account key from the master public key;

deriving a third public transaction key from the third public account key;

deriving, using a hashing function, a multi-approval transaction address for a distributed ledger in a customer wallet from the first public transaction key derived from a first public account key, the second public transaction key, and the third public transaction key; and

transmitting the multi-approval transaction address to a customer device.

12. The computerized method of claim 11, wherein the first public transaction key, the second public transaction key, and the third public transaction key are non-extended keys.

13. The computerized method of claim 11, wherein the customer device requires private keys corresponding to at least two of the first public transaction key, the second public transaction key, and the third public transaction key in order to transact from the multi-approval transaction address.

14. The computerized method of claim 13, further comprising:

communicating a private key associated with the second public transaction key to the customer device.

15. The computerized method of claim 11, further comprising verifying, at the computing device, identity data from the customer device at least in part by:

comparing the identity data with stored identity data for a customer.

16. The computerized method of claim 15, wherein the identity data comprises biometric data.

17. The computerized method of claim 11, further comprising receiving the master public key from at least one of a credit union or a bank.

18. The computerized method of claim 11, wherein the customer wallet stores at least one of a security, a currency, a commodity, a bond, a fund, or a combination thereof.

19. The computerized method of claim 11, further comprising:

determining the first public transaction key that was derived from the first public account key;

determining the second public transaction key that was derived from the second public account key; and

determining the third public transaction key that was derived from the third public account key.

20. The computerized method of claim 11, further comprising:

producing a signed transaction by signing a transaction that transacts from the multi-approval transaction address to multiple output addresses, wherein the customer device signs the transaction using respective private keys associated with at least two of:

the first public transaction key;

the second public transaction key; and

the third public transaction key; and

sending the signed transaction across a network for recording on the distributed ledger.