

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 ~~communicate with a customer device and a trusted third party~~ 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 ~~a the first public transaction key derived from a first parent public account key, a the second public key derived from a second parent public transaction key, and a the third public key derived from a third parent public key;~~ 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 key is a public transaction key received from the customer device, wherein the second public key is a public transaction key derived from the second parent public key stored at the computing device, wherein the third public key is a public transaction key derived from a third parent public key received from the trusted third party.~~

32. The computing system of claim 21, wherein the first public transaction key, the second public transaction key, and the third public transaction key are non-extended keys.

43. 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.

54. The computing system of claim 43, 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.

65. The computing system of claim 1, wherein the at least one processor is configured to verify ~~identify~~ identity data from the customer device at least in part by: comparing the identity data with ~~previously~~ stored identity data for ~~the a~~ customer.

76. The computing system of claim 65, wherein the identity data comprises biometric data.

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

98. The computing system of claim 1, wherein the customer wallet ~~is used to store~~ stores at least one of a security, a currency, a commodity, a bond, a fund, or a combination thereof.

109. The computing system of claim 1, wherein the at least one processor is further configured to:
determine the first public transaction key that ~~is~~ was derived from the first ~~parent~~ public account key;
determine the second public transaction key that ~~is~~ was derived from the second ~~parent~~ public account key; and

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

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

produce 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 a respective private key associated with 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. The computing system of claim 1, wherein the third public account key corresponds to a first customer and at least one other public account key corresponds to at least one other customer.

11. — A system comprising:

~~— a computing device configured to communicate with a customer device for a customer; and~~

~~wherein the computing device is configured to derive, using a hashing function, a multi-approval transaction address in a customer wallet from a first public key derived from a first parent public key, a second public key derived from a second parent public key, and a third public key derived from a third parent public key; and~~

~~— wherein the computing device is configured to transmit the multi-approval transaction address to the customer device.~~

12. — The system of claim 11, wherein the first public key is a public transaction key received from the customer device, wherein the second public key is a public transaction key derived from the second parent public key stored at the computing device, wherein the third public key is a public transaction key derived from the third parent public key received from a trusted third party.

13. ~~The system of claim 12, wherein the first public key, the second public key, and the third public key are non-extended keys.~~
14. ~~The system of claim 11, wherein the customer device requires private keys corresponding to at least two of the first public key, the second public key, and the third public key in order to transact from the multi-approval transaction address.~~
15. ~~The system of claim 14, wherein the computing device is further configured to: communicate a private key associated with the second public key to the customer device.~~
16. ~~The system of claim 11, wherein the computing device is configured to verify identify data from the customer device at least in part by: ~~comparing the identity data with previously stored identity data for the customer.~~~~
17. ~~The system of claim 16, wherein the identity data comprises biometric data.~~
18. ~~The system of claim 12, wherein the trusted third party is at least one of a credit union or a bank.~~
19. ~~The system of claim 11, wherein the customer wallet is used to store at least one of a security, a currency, a commodity, a bond, a fund, or a combination thereof.~~
20. ~~The system of claim 11,~~
~~wherein the computing device is configured to determine the first public key that is derived from the first parent public key;~~
~~wherein the computing device is configured to determine the second public key that is derived from the second parent public key; and~~
~~wherein the computing device is configured to determine the third public key that is derived from the third parent public key.~~

2412. 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 a-the first public transaction key derived from a first parent-public account key, a-the second public key derived from a second parent public transaction key, and a-the third public key derived from a first parent public transaction key; and

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

22. — ~~The computerized method of claim 21, wherein the first public key is a public transaction key received from the customer device, wherein the second public key is a public transaction key derived from the second parent public key stored at the computing device, wherein the third public key is a public transaction key derived from the third parent public key received from a trusted third party.~~

2313. The computerized method of claim 2212, wherein the first public transaction key, the second public transaction key, and the third public transaction key are non-extended keys.

2414. The computerized method of claim 2412, 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.

2515. The computerized method of claim 2414, further comprising:

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

2616. The computerized method of claim 2412, further comprising verifying, at the computing device, identity data from the customer device at least in part by:

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

2717. The computerized method of claim 2616, wherein the identity data comprises biometric data.

2818. The computerized method of claim 2212, ~~wherein~~ further comprising receiving the trusted third party is master public key from at least one of a credit union or a bank.

2919. The computerized method of claim 2412, wherein the customer wallet ~~is used to store~~ stores at least one of a security, a currency, a commodity, a bond, a fund, or a combination thereof.

3020. The computerized method of claim 2412, further comprising:

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

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

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

21. The computerized method of claim 12, 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 a respective private key associated with 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.

22. The computerized method of claim 12, wherein the third public account key corresponds to a first customer and at least one other public account key corresponds to at least one other customer.