

CLAIMS

1. A computing system comprising:
 - at least one processor;
 - at least one memory communicatively coupled to the at least one processor;
 - at least one network interface communicatively coupled to the at least one processorand configured to communicate with a customer device and a trusted third party;
 - wherein the at least one processor 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;
 - 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.
3. The computing system of claim 2, wherein the first public key, the second public key, and the third public key are non-extended keys.
4. The computing system of claim 1, 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.
5. The computing system of claim 4, wherein the at least one network interface is configured to:
 - communicate a private key associated with the second public key to the customer device.
6. The computing system of claim 1, wherein the at least one processor 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.

7. The computing system of claim 6, wherein the identity data comprises biometric data.
8. The computing system of claim 1, wherein the trusted third party is at least one of a credit union or a bank.
9. The computing system of claim 1, 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.
10. The computing system of claim 1, wherein the at least one processor is further configured to:
 - determine the first public key that is derived from the first parent public key;
 - determine the second public key that is derived from the second parent public key;
 - and
 - determine the third public key that is derived from the third parent public key.
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 identity 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.
21. A computerized method comprising:
deriving, 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 first parent public 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.

23. The computerized method of claim 22, wherein the first public key, the second public key, and the third public key are non-extended keys.

24. The computerized method of claim 21, 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.

25. The computerized method of claim 24, further comprising:
communicating a private key associated with the second public key to the customer device.

26. The computerized method of claim 21, 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 customer.

27. The computerized method of claim 26, wherein the identity data comprises biometric data.

28. The computerized method of claim 22, wherein the trusted third party is at least one of a credit union or a bank.

29. The computerized method of claim 21, 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.

30. The computerized method of claim 21, further comprising:
- determining the first public key that is derived from the first parent public key;
 - determining the second public key that is derived from the second parent public key;
- and
- determining the third public key that is derived from the third parent public key.