

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 processor and configured to communicate with a customer device and a trusted third party;
 - wherein the at least one network interface is configured to receive, from the customer device, identity data for a customer and a request to restore a customer wallet;
 - wherein the at least one processor is configured to:
 - derive a second key from a cryptographic master key associated with wallets of multiple customers, wherein the second key is associated with the customer wallet; and
 - verify the identity data for the customer received from the customer device; and
 - when the at least one processor verifies the identity data for the customer received from the customer device, the at least one network interface is configured to communicate a request for a first key associated with the customer wallet to a key repository for the trusted third party; and
 - wherein the at least one processor is configured to restore the customer wallet using the first key associated with the customer wallet and a-the second key associated with the customer wallet.
2. The computing system of claim 1, further comprising:
 - when the at least one network interface receives the first key associated with the customer wallet from the key repository for the trusted third party, the at least one processor is configured to restore the customer wallet using the first key associated with the customer wallet and the second key associated with the customer wallet.
3. The computing system of claim 2, wherein the at least one processor is configured to restore the customer wallet using the first key associated with the customer wallet and the second key associated with the customer wallet at least in part by:

generating one or more new private keys associated with a new customer wallet;
generating a new transaction address associated with the new customer wallet based on the one or more new private keys; and
transferring digital assets from the old customer wallet to the new transaction address using the first key and the second key.

4. The computing system of claim 3,

wherein the customer wallet comprises a plurality of old transaction addresses, each respective old transaction address of the plurality of old transaction addresses being associated with three respective private keys, and

wherein each respective old transaction address of the plurality of old transaction addresses requires at least two respective private keys of the three respective ~~three~~ private keys associated with the respective old transaction address to access any digital assets in the respective old transaction address.

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

communicate the new transaction address associated with the new customer wallet to the customer device.

6. The computing system of claim 5, wherein the at least one network interface is configured to:

communicate at least one of the one or more of the new private keys to the customer device.

7. The computing system of claim 6, wherein the one or more new private keys are private transaction keys.

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

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

9. The computing system of claim 1, wherein the identity data comprises biometric data.

10. The computing system of claim 1, wherein the trusted third party is at least one of a credit union or a bank.

11. 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.

2312. A computerized method comprising:

deriving a second key from a cryptographic master key associated with wallets of multiple customers, wherein the second key is associated with a customer wallet;

receiving, at a computing device, identity data for a customer and a request to restore ~~a~~ the customer wallet from a customer device;

verifying, at the computing device, the identity data for the customer received from the customer device;

when the identity data for the customer received from the customer device is verified, communicating a request for a first key associated with the customer wallet to a key repository for a trusted third party; and

receiving the first key associated with the customer wallet from the key repository for the trusted third party; ~~and~~

wherein the customer wallet can be restored using the first key associated with the customer wallet and ~~a~~ the second key associated with the customer wallet.

2413. The computerized method of claim 2312, further comprising:

restoring the customer wallet at the computing device using the first key associated with the customer wallet and the second key associated with the customer wallet.

[2514](#). The computerized method of claim [2413](#), wherein restoring the customer wallet at the computing device using the first key associated with the customer wallet and the second key associated with the customer wallet comprises:

generating one or more new private keys associated with a new customer wallet;
generating a new transaction address associated with the new customer wallet based on the one or more new private keys; and
transferring digital assets from the old customer wallet to the new transaction address using the first key and the second key.

[2615](#). The computerized method of claim [2514](#),

wherein the customer wallet comprises a plurality of old transaction addresses, each [respective old transaction address of the plurality of old transaction addresses](#) being associated with three [respective](#) private keys, [and](#)

wherein each [respective](#) old transaction address [of the plurality of old transaction addresses](#) requires at least two [respective private keys](#) of the [three](#) respective ~~three~~ private keys associated with the respective old transaction address to access any digital assets in the respective old transaction address.

[2716](#). The computerized method of claim [2514](#), further comprising:

communicating the new transaction address associated with the new customer wallet to the customer device.

[2817](#). The computerized method of claim [2514](#), further comprising:

communicating [at least one of the](#) one or more of the new private keys to the customer device.

[2918](#). The computerized method of claim [2817](#), wherein the [one or more](#) new private keys are private transaction keys.

[3019](#). The computerized method of claim [2312](#), wherein verifying, at the computing device, the identity data for the customer received from the customer device comprises:
comparing the identity data with previously stored identity data for the customer.

[3120](#). The computerized method of claim [2312](#), wherein the identity data comprises biometric data.

[3221](#). The computerized method of claim [2312](#), wherein the trusted third party is at least one of a credit union or a bank.

[3322](#). The computerized method of claim [2312](#), 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.

~~12. — A system comprising:~~

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

~~—— a key repository communicatively coupled with the computing device;~~

~~—— wherein the computing device is configured to receive, from a customer device, identity data for a customer and a request to restore a customer wallet;~~

~~—— wherein the computing device is configured to verify the identity data for the customer received from the customer device;~~

~~—— wherein the computing device is configured to communicate a request for a first key associated with the customer wallet to a key repository for the trusted third party; and~~

~~—— wherein the computing device restores the customer wallet using the first key associated with the customer wallet and a second key associated with the customer wallet.~~

~~13. — The system of claim 12, further comprising:~~

—when the computing device receives the first key associated with the customer wallet from the key repository for the trusted third party, the computing device is configured to restore the customer wallet using the first key associated with the customer wallet and the second key associated with the customer wallet.

14. The system of claim 13, wherein the computing device is configured to restore the customer wallet using the first key associated with the customer wallet and the second key associated with the customer wallet at least in part by:

—generating one or more new private keys associated with a new customer wallet;
generating a new transaction address associated with the new customer wallet based on the one or more new private keys; and
transferring digital assets from the old customer wallet to the new transaction address using the first key and the second key.

15. The system of claim 14,

wherein the customer wallet comprises a plurality of old transaction addresses, each being associated with three private keys,

wherein each old transaction address requires at least two of the respective three private keys associated with the respective old transaction address to access any digital assets in the respective old transaction address.

16. The system of claim 14, wherein the computing device is further configured to:

—communicate the new transaction address associated with the new customer wallet to the customer device.

17. The system of claim 16, wherein the computing device is further configured to:

—communicate one or more of the new private keys to the customer device.

18. The system of claim 17, wherein the new private keys are private transaction keys.

19. — ~~The system of claim 12, wherein the computing device is configured to verify the identify data for the customer received from the customer device at least in part by:~~

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

20. — ~~The system of claim 12, wherein the identity data comprises biometric data.~~

21. — ~~The system of claim 12, wherein the trusted third party is at least one of a credit union or a bank.~~

22. — ~~The system of claim 12, 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.~~