

CLAIMS

1. A system comprising:
 - a first user computing device;
 - at least one remotely located computing device configured to communicate with the first user computing device;
 - wherein the at least one remotely located computing device is configured to communicate a plurality of public encryption keys to the first user computing device;
 - wherein the first user computing device is configured to:
 - split at least one secret into a plurality of shares, wherein at least a subset of the plurality of shares is sufficient to reconstruct the at least one secret;
 - generate a respective hash for each respective share of the plurality of shares;
 - encrypt each of the plurality of shares based on a different public encryption key of the plurality of public encryption keys to create a plurality of encrypted shares;
 - and
 - communicate the plurality of encrypted shares and the respective hash for each respective share of the plurality of shares to the at least one remotely located computing device; and
 - wherein the at least one remotely located computing device is configured to:
 - store the plurality of encrypted shares;
 - transfer, via at least one mobile storage device, each respective encrypted share of the plurality of encrypted shares to a respective trusted computing device of a plurality of trusted computing devices;
 - transfer each respective hash for each respective share of the plurality of shares to a respective trusted computing device of the plurality of trusted computing devices;
 - wherein each of the plurality of trusted computing devices is configured to:
 - decrypt a respective encrypted share into a respective un-encrypted share;
 - generate a respective recovery hash from the respective un-encrypted share;
 - and
 - verify that the respective un-encrypted share matches one of the plurality of shares before it was encrypted at least in part by comparing the respective hash with the respective recovery hash to determine whether data in the respective un-encrypted share is accurate.

2. The system of claim 1, wherein the first user computing device is further configured to sign each of the plurality of encrypted shares using a private signature key.
3. The system of claim 1, wherein the first user computing device is configured to encrypt using an Elliptic Curve Diffie Hellman (ECDH) operation, comprising:
 - determining a plurality of ECDH keys, each determined based on a private signature key and a respective public encryption key of the plurality of public encryption keys;
 - determining a plurality of Advanced Encryption Standard (AES) keys, each determined as a hash of a respective ECDH key, a public signature key, and the respective public encryption key of the plurality of public encryption keys; and
 - encrypting each of the plurality of shares, along with a respective AES key, into a respective encrypted share of the plurality of encrypted shares.
4. The system of claim 1, wherein each different public encryption key of the plurality of public encryption keys is derived using a Hierarchical Deterministic (HD) methodology from a different master seed key.
5. The system of claim 1, wherein the plurality of shares are Shamir secret shares.
6. The system of claim 1, wherein the first user computing device is configured to split the at least one secret into the plurality of shares through at least one of polynomial interpolation or Shamir secret sharing.
7. The system of claim 1, wherein the plurality of shares are Shamir secret shares; and wherein the first user computing device is configured to split the at least one secret into the plurality of shares using Shamir secret sharing.
8. The system of claim 1, wherein the at least one secret includes at least one of: a key, a cryptographic key, a private key, a public encryption key, an encryption key, a signature key, and a password.
9. The system of claim 1, wherein the at least one secret is used to encrypt data, decrypt data, and sign transactions.

10. The system of claim 1, wherein the plurality of public encryption keys are each part of a different encryption key pair with a different private key, each different private key stored on a different computing device.
11. The system of claim 10, wherein each different computing device is controlled by a different group of individuals.
12. The system of claim 10, wherein each different computing device is located at a different physical location from other different computing devices.
13. The system of claim 3, further comprising:
a second user computing device;
wherein the second user computing device is configured to communicate at least one recovery public encryption key to the at least one remotely located computing device;
wherein the at least one remotely located computing device is configured to communicate at least one recovery encrypted share to the second user computing device;
wherein the second user computing device is configured to decrypt each of the at least one recovery encrypted share to create a first plurality of un-encrypted shares based on at least one recovery private decryption key corresponding to the at least one recovery public encryption key; and
wherein the second user computing device is configured to reconstruct the at least one secret using the first plurality of un-encrypted shares.
14. The system of claim 13, wherein each different recovery public encryption key of the at least one recovery public encryption key is part of a different recovery encryption key pair with a different recovery private decryption key of the at least one recovery private decryption key.
15. The system of claim 13, wherein the at least one recovery private decryption key is a single recovery private decryption key; and
wherein the at least one recovery public encryption key is a single recovery public encryption key.

16. The system of claim 15, wherein each of the plurality of trusted computing devices is configured to decrypt using a second Elliptic Curve Diffie Hellman (ECDH) operation, comprising:

- determining at least one recovery ECDH key, each determined based on a respective recovery public signature key and a respective recovery private decryption key of the at least one recovery private decryption key;

- for each respective recovery ECDH key of the at least one recovery ECDH key, determining an Advanced Encryption Standard (AES) key as a hash of the respective recovery ECDH key, the respective recovery public signature key, and a respective recovery public encryption key; and

- decrypt each of the at least one recovery encrypted share, combined with a corresponding recovery AES key, into a respective un-encrypted share of the first plurality of un-encrypted shares.

17. A computerized method comprising:

- communicating a plurality of public encryption keys from at least one remotely located computing device to a first user computing device;

- splitting at least one secret into a plurality of shares at the first user computing device, wherein at least a subset of the plurality of shares is sufficient to reconstruct the at least one secret;

- generating, at the first user computing device, a respective hash for each respective share of the plurality of shares;

- encrypting each of the plurality of shares based on a different public encryption key of the plurality of public encryption keys at the first user computing device to create a plurality of encrypted shares;

- communicating the plurality of encrypted shares from the first user computing device to the at least one remotely located computing device; and

- communicating the respective hash for each respective share of the plurality of shares to the at least one remotely located computing device;

- storing the plurality of encrypted shares at the at least one remotely located computing device;

- transferring, via at least one mobile storage device, each of the plurality of encrypted shares from the at least one remotely located computing device to a respective trusted computing device of a plurality of trusted computing devices;

transferring each respective hash for each respective share of the plurality of shares from the at least one remotely located computing device to a respective trusted computing device of the plurality of trusted computing devices;

decrypting, at each trusted computing device, a respective encrypted share into a respective un-encrypted share;

generating, at each trusted computing device, a respective recovery hash from the respective un-encrypted share; and

verifying, at each trusted computing device, that the respective un-encrypted share matches one of the plurality of shares before it was encrypted at least in part by comparing the respective hash with the respective recovery hash to determine whether data in the respective un-encrypted share is accurate.

18. The computerized method of claim 17, wherein decrypting comprises using an Elliptic Curve Diffie Hellman (ECDH) operation, comprising:

determining at least one recovery ECDH key, each determined based on a respective recovery public signature key and at least one recovery private decryption key;

for each respective recovery ECDH key of the at least one recovery ECDH key, determining an Advanced Encryption Standard (AES) key as a hash of the respective recovery ECDH key, the respective recovery public signature key, and a respective recovery public encryption key; and

decrypt each encrypted share, combined with a corresponding recovery AES key, into the respective un-encrypted share.

19. The computerized method of claim 17, further comprising:

re-encrypting a plurality of un-encrypted shares into recovery encrypted shares;

transferring the plurality of un-encrypted shares to the at least one remotely located computing device;

communicating the recovery encrypted shares to a second user computing device from the at least one remotely located computing device;

decrypting each of the recovery encrypted shares at the second user computing device to create a plurality of decrypted shares; and

reconstructing the at least one secret at the second user computing device using the plurality of decrypted shares.

20. The computerized method of claim 19, wherein re-encrypting comprises using an Elliptic Curve Diffie Hellman (ECDH) operation, comprising:

determining a plurality of recovery ECDH keys, each determined based on a respective recovery private signature key and a respective recovery public encryption key;

determining a plurality of Advanced Encryption Standard (AES) keys, each determined as a hash of a respective recovery ECDH key, a respective recovery public signature key, and the respective recovery public encryption key; and

encrypting each of a plurality of un-encrypted shares, along with a respective AES key, into a respective recovery encrypted share of the recovery encrypted shares.