

CLAIMS

What is claimed is:

1. A computing device comprising:
at least one processor; and
at least one memory communicatively coupled to the at least one processor;
wherein the at least one processor is configured to:
determine a secret to be protected;
split the secret into a plurality of secret shares, at least a subset of which are required to reconstitute the secret;
transfer each secret share to a respective portable storage device or media for distribution to a respective shareholder;
generate metadata with at least a hash of each secret share; and
store the metadata separate from the portable storage devices or media with the secret shares.
2. The computing device of claim 1, wherein each of the secret, the secret shares, and the hashes of the secret shares are a different string of characters.
3. The computing device of claim 1, wherein the secret is a cryptographic private key or a mnemonic phrase or seed that can be used to reconstitute a private key.
4. The computing device of claim 1, wherein the at least one processor is configured to split the secret into the plurality of secret shares using Shamir secret sharing or polynomial interpolation.
5. The computing device of claim 1,
wherein the at least one processor is configured to verify the secret shares by using each secret share at least once to reconstitute the secret, and
wherein the secret shares are only transferred to their respective portable storage devices or media after the secret shares are successfully verified.
6. The computing device of claim 1, wherein the at least one processor is configured to:

before determining the secret, erase contents of at least one storage device and perform a clean installation of an operating system in the computing device; and after transferring each secret share to a respective portable storage devices or media, delete any locally-stored copies of the secret and the secret shares on the computing device.

7. The computing device of claim 1,
wherein the secret is a cryptographic private key or a mnemonic phrase or seed that can be used to recover the cryptographic private key,
wherein the at least one processor is configured to determine the secret by generating the cryptographic private key or mnemonic phrase or seed.
8. The computing device of claim 7,
wherein the at least one processor also generates the following information in the metadata:
 - a public key that corresponds to the cryptographic private key; and
 - at least one address in a distributed ledger.
9. The computing device of claim 1, wherein the at least one processor is configured to:
determine retrieved secret shares from at least two secret share storage devices or media that are retrieved from the shareholders; and
attempt to reconstitute the secret using the retrieved secret shares from the at least two secret share storage devices or media.
10. The computing device of claim 9, wherein the at least one processor is configured to:
when the secret cannot be reconstituted from the retrieved secret shares, identify at least one of the retrieved secret shares as being incorrect based on the metadata.
11. A method for secret splitting and metadata storage, comprising:
 - determining a secret to be protected;
 - splitting the secret into a plurality of secret shares, at least a subset of which are required to reconstitute the secret;
 - transferring each secret share to a respective portable storage device or media for distribution to a respective shareholder;
 - generating metadata with at least a hash of each secret share; and

storing the metadata separate from the portable storage devices or media with the secret shares.

12. The method of claim 11, wherein each of the secret, the secret shares, and the hashes of the secret shares are a different string of characters.

13. The method of claim 11, wherein the secret is a cryptographic private key or a mnemonic phrase or seed that can be used to reconstitute a private key.

14. The method of claim 11, wherein the splitting comprises splitting the secret into the plurality of secret shares using Shamir secret sharing or polynomial interpolation.

15. The method of claim 11, further comprising verifying the secret shares by using each secret share at least once to reconstitute the secret, and
wherein the secret shares are only transferred to their respective portable storage devices or media after the secret shares are successfully verified.

16. The method of claim 11, further comprising:
before determining the secret, erase contents of at least one storage device and perform a clean installation of an operating system in a computing device; and
after transferring each secret share to a respective portable storage devices or media, delete any locally-stored copies of the secret and the secret shares on the computing device.

17. The method of claim 11,
wherein the secret is a cryptographic private key or a mnemonic phrase or seed that can be used to recover the cryptographic private key,
wherein the secret is determined by generating the cryptographic private key or mnemonic phrase or seed.

18. The method of claim 17, further comprising generating the following information in the metadata:
a public key that corresponds to the cryptographic private key; and
at least one address in a distributed ledger.

19. The method of claim 11, further comprising:
 - determining a retrieved secret share from each of at least two secret share storage devices or media that are retrieved from the shareholders; and
 - attempting to reconstitute the secret using the retrieved secret shares from the at least two secret share storage devices or media.
20. The method of claim 19, further comprising, when the secret cannot be reconstituted from the retrieved secret shares, identify at least one of the retrieved secret shares as being incorrect based on the metadata.
21. A computing device comprising:
 - at least one processor; and
 - at least one memory communicatively coupled to the at least one processor;wherein the at least one processor is configured to:
 - determine a retrieved secret share from each of at least two secret share storage devices or media that are retrieved from at least two of a plurality of shareholders;
 - determine metadata, the metadata having at least a list of hashes of a plurality of secret shares that were generated before the secret shares were distributed to the plurality of shareholders;
 - attempt to reconstitute the secret using the retrieved secret shares from the at least two secret share storage devices or media; and
 - when the secret cannot be reconstituted from the retrieved secret shares, identify at least one of the retrieved secret shares as being incorrect based on the metadata.
22. The computing device of claim 21, wherein each of the secret, the retrieved secret shares, and the hashes of the plurality of secret shares are a different string of characters.
23. The computing device of claim 21, wherein the secret is a cryptographic private key or a mnemonic phrase or seed that can be used to reconstitute a private key.
24. The computing device of claim 21, wherein the at least one processor is configured to attempt to reconstitute the secret using Shamir combining.

25. The computing device of claim 21,
wherein the at least one processor is configured to verify each of the retrieved secret shares by comparing the respective retrieved secret share to the list of hashes in the metadata, and
wherein, when a respective retrieved secret share matches a hash in the list of hashes in the metadata, the respective retrieved secret share is successfully verified.
26. The computing device of claim 25, wherein the at least one processor is configured to attempt to reconstitute the secret only after the secret shares are successfully verified.
27. The computing device of claim 21, wherein the at least one processor is configured to, when the secret is reconstituted from the retrieved secret shares, perform at least one of the following actions requiring the reconstituted secret:
encrypting or decrypting data using the reconstituted secret;
generating a transaction address in a distributed ledger based on the reconstituted secret; or
signing a transaction using the reconstituted secret, wherein the transaction sends cryptocurrency out of an address in the distributed ledger.
28. The computing device of claim 21, wherein the at least one processor is configured to, before the retrieved secret shares are determined:
split the secret into the plurality of secret shares, at least a subset of which are required to reconstitute the secret; and
transfer each secret share to a respective portable storage device or media;
wherein each portable storage device or media is distributed to the plurality of shareholders.
29. A method, comprising:
determining a retrieved secret share from each of at least two secret share storage devices or media that are retrieved from at least two of a plurality of shareholders;
determining metadata, the metadata having at least a list of hashes of a plurality of secret shares that were generated before the secret shares were distributed to the plurality of shareholders;

attempting to reconstitute the secret using the retrieved secret shares from the at least two secret share storage devices or media; and

when the secret cannot be reconstituted from the retrieved secret shares, identifying at least one of the retrieved secret shares as being incorrect based on the metadata.

30. The method of claim 29, wherein each of the secret, the retrieved secret shares, and the hashes of the plurality of secret shares are a different string of characters.

31. The method of claim 29, wherein the secret is a cryptographic private key or a mnemonic phrase or seed that can be used to reconstitute a private key.

32. The method of claim 29, further comprising attempting to reconstitute the secret using Shamir combining.

33. The method of claim 29, further comprising verifying each of the retrieved secret shares by comparing the respective retrieved secret share to the list of hashes in the metadata, wherein, when a respective retrieved secret share matches a hash in the list of hashes in the metadata, the respective retrieved secret share is successfully verified.

34. The method of claim 33, wherein the attempting comprises attempting to reconstitute the secret only after the secret shares are successfully verified.

35. The method of claim 29, further comprising, when the secret is reconstituted from the retrieved secret shares, performing at least one of the following actions requiring the reconstituted secret:

encrypting or decrypting data using the reconstituted secret;

generating a transaction address in a distributed ledger based on the reconstituted secret; or

signing a transaction using the reconstituted secret, wherein the transaction sends cryptocurrency out of an address in the distributed ledger.

36. The method of claim 29, further comprising, before the retrieved secret shares are determined:

splitting the secret into the plurality of secret shares, at least a subset of which are required to reconstitute the secret; and

transferring each secret share to a respective portable storage device or media;

wherein each portable storage device or media is distributed to the plurality of shareholders.