

CLAIMS

What is claimed is:

1. A system comprising:
 - at least one processor; and
 - at least one memory communicatively coupled to the at least one processor; ~~and~~
 - wherein the at least one processor is configured to:
 - encrypt each corresponding secret part of at least one set of secret parts into a corresponding singly-encrypted secret part using at least one corresponding symmetric key to produce the corresponding singly-encrypted secret part; and
 - encrypt each corresponding singly-encrypted secret part into a corresponding doubly-encrypted secret part using a corresponding at least one public key, the corresponding at least one ~~each~~ public key belonging to a corresponding ~~one of at least one~~ public/private keypair; and
 - wherein ~~at least a subset of the secret parts of the at least one set of~~ two or more ~~doubly-encrypted~~ secret parts are used to reconstruct a secret.
- ~~2. The system of claim 1, wherein each secret part is encrypted into a corresponding singly encrypted secret part using at least one corresponding symmetric key.~~
- ~~3. The system of claim 2, wherein the at least one corresponding symmetric key for a first secret part and a second secret part is identical.~~
- ~~4. The system of claim 2, wherein the at least one corresponding symmetric key for a first secret part and a second secret part is distinct.~~
- ~~5. The system of claim 1, wherein each secret part is encrypted into a corresponding singly encrypted secret part using the corresponding at least one public key belonging to the corresponding one of the at least one public/private keypair.~~
6. The system of claim 1,
 - wherein each corresponding singly-encrypted secret part is encrypted using a single ~~the at least one~~ public key is a single public key used to encrypt all the singly-encrypted ~~secret parts~~, the single public key belonging to a single public/private keypair; and

wherein the ~~at least one private key is a single private key belonging to the single~~ public/private keypair also includes a corresponding private key.

~~73.~~ The system of claim 1, wherein the at least one processor is further configured to:
decrypt ~~at least one of the each~~ doubly-encrypted secret parts into ~~at least one of the~~ corresponding singly-encrypted secret parts using a corresponding at least one private key, each belonging to a the corresponding ~~one of the at least one~~ public/private keypair; and
re-encrypt each ~~of the at least one corresponding~~ singly-encrypted secret part using a corresponding second public key, the corresponding second public key belonging to a second public/private keypair.

~~84.~~ The system of claim 1, wherein the at least one processor is configured to encrypt each secret part by exclusive ORing (XORing) each secret part with the at least one corresponding symmetric key to produce the corresponding singly-encrypted secret part.

~~95.~~ The system of claim 1, wherein each doubly-encrypted secret part is encrypted using both at least one symmetric key and ~~the a~~ a public key ~~corresponding~~ belonging to the corresponding ~~one of the at least one~~ public/private keypair.

~~106.~~ The system of claim 1, wherein each doubly-encrypted secret part is encrypted twice using ~~the a~~ a public key corresponding belonging to the corresponding ~~one of the at least one~~ public/private keypair.

~~117.~~ The system of claim 1, wherein each doubly-encrypted secret part is encrypted using both at least one symmetric key and ~~the a~~ a corresponding part holder public key belonging to a corresponding part holder public/private keypair.

~~128.~~ The system of claim 1, wherein the at least one processor is further configured to:
receive ~~a plurality of the~~ two or more doubly-encrypted secret parts;
decrypt each of the ~~plurality of~~ two or more doubly-encrypted secret parts into the corresponding singly-encrypted secret part using a corresponding private key belonging to the corresponding ~~one of the at least one~~ public/private keypair;
decrypt each corresponding singly-encrypted secret part into ~~the a~~ a corresponding secret part; and

reconstruct ~~a~~the secret from a quantity of ~~the~~ corresponding secret parts, wherein the quantity is a subset of a total number of secret parts previously created from the secret.

~~139.~~ The system of claim ~~128~~,
wherein each corresponding doubly-encrypted secret part is distributed to a respective part holder of a plurality of part holders; ~~and~~
wherein the ~~plurality of two or more~~ doubly-encrypted secret parts are received from two or more part holders of the a plurality of the part holders.

~~1410.~~ The system of claim 1, wherein the at least one processor is further configured to:
reconstruct ~~a~~the secret from a plurality of ~~the~~ secret parts, wherein the secret is a symmetric encryption key; and
perform an action with the ~~asset~~symmetric encryption key.

~~1511.~~ The system of claim ~~1410~~, wherein the action comprises at least one of the following actions using the ~~reconstructed~~ secret reconstructed from the two or more doubly-encrypted secret parts:
encrypting first data;
decrypting second data;
generating a transaction address; or
signing a transaction.

12. The system of claim 1, wherein the at least one processor is further configured to periodically determine and store new versions of at least one of the following:
the at least one corresponding symmetric key;
the corresponding at least one public key belonging to the corresponding public/private keypair;
corresponding at least one private key belonging to the corresponding public/private keypair; or
some combination of the at least one corresponding symmetric key, the corresponding at least one public key, and the corresponding at least one private key.

13. The system of claim 1, wherein the two or more doubly-encrypted secret parts are received at an air-gapped computing device that reconstructs the secret using the two or more doubly-encrypted secret parts.

~~16~~14. A system comprising:

at least one processor; and

at least one memory communicatively coupled to the at least one processor; ~~and~~

wherein the at least one processor is configured to:

receive a plurality of doubly-encrypted secret parts that were encrypted using at least a public key belonging to a public/private keypair;

decrypt each of the plurality of doubly-encrypted secret parts into a corresponding singly-encrypted secret part using a private key belonging to the public/private keypair; and

decrypt each corresponding singly-encrypted secret part into a corresponding secret part using at least one corresponding symmetric key; and

wherein a secret is reconstructed from a quantity of corresponding secret parts that is a subset of a total number of secret parts previously created from the secret.

~~17. The system of claim 16, wherein each doubly-encrypted secret part was encrypted into a corresponding singly-encrypted secret part using at least one corresponding symmetric key.~~

~~18. The system of claim 17, wherein the at least one symmetric key for a first secret part and a second secret part is identical.~~

~~19. The system of claim 17, wherein the at least one symmetric key for at a first secret part and a second secret part is distinct.~~

~~20~~15. The system of claim ~~16~~14, wherein each doubly-encrypted secret part was encrypted using two stages, comprising:

a first stage during which ~~a~~each corresponding secret part was encrypted into ~~a~~the corresponding singly-encrypted secret part using a symmetric key or the public key belonging to the public/private keypair; and

a second stage during which the corresponding singly-encrypted secret part was encrypted into ~~the~~ a respective doubly-encrypted secret part using ~~a~~ the public key belonging to a corresponding public/private keypair.

~~21~~16. The system of claim ~~16~~14, wherein the at least one processor is further configured to perform at least one of the following actions using the ~~reconstructed~~-secret reconstructed from the quantity of the total number of secret parts:

- encrypting first data;
- decrypting second data;
- generating a transaction address; or
- signing a transaction.

~~22~~17. The system of claim ~~16~~14, wherein the at least one processor is configured to decrypt each corresponding singly-encrypted secret part by exclusive ORing (XORing) each corresponding singly-encrypted secret part with the at least one corresponding symmetric key to produce the corresponding secret part.

~~23~~18. The system of claim ~~16~~14, wherein the plurality of doubly-encrypted secret parts are received from a plurality of part holders.

19. The system of claims 1 or 14, wherein the at least one corresponding symmetric key for a first secret part and a second secret part is identical.

20. The system of claims 1 or 14, wherein the at least one corresponding symmetric key for a first secret part and a second secret part is distinct.

~~24~~21. A method for securely distributing secret parts to a plurality of part holders, comprising:

- encrypting each secret part of at least one set of secret parts into a corresponding singly-encrypted secret part using at least one symmetric key ~~or a corresponding one of at least one public key, each public key belonging to a corresponding one of at least one public/private keypair;~~

encrypting each corresponding singly-encrypted secret part into a corresponding doubly-encrypted secret part using ~~the~~ a corresponding at least one public key belonging to ~~the~~ a corresponding public/private keypair; and

distributing each doubly-encrypted secret part to a respective part holder;

wherein ~~at least a subset of the secret parts of the~~ at least one set of two or more doubly-encrypted secret parts are used to reconstruct a secret.

22. A method for reconstructing an asset encryption key, comprising:

receiving a plurality of doubly-encrypted secret parts that were encrypted using at least a public key belonging to a public/private keypair;

decrypting each of the plurality of doubly-encrypted secret parts into a corresponding singly-encrypted secret part using a private key belonging to the public/private keypair; and

decrypting each corresponding singly-encrypted secret part into a corresponding secret part using at least one corresponding symmetric key;

wherein a secret is reconstructed from a quantity of corresponding secret parts that is a subset of a total number of secret parts previously created from the secret.