

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;
wherein the at least one processor is configured to:
encrypt at least one set of asset encryption key parts into at least one set of encrypted asset encryption key parts using at least one of:
at least one symmetric key; or
at least one public key of at least one public/private keypair associated with the system;
wherein at least a subset of the at least one set of asset encryption key parts are used to reconstruct an asset encryption key, which is used to perform an action using at least one asset key.
2. The system of claim 1, wherein using at least one of the at least one symmetric key or the at least one public key of the at least one public/private keypair associated with the system includes:
using the at least one public key of the at least one public/private keypair associated with the system when the system implements an online signing service,
wherein at least one private key, corresponding to the at least one public key of the at least one public/private keypair associated with the system, is stored in the at least one memory in the system.
3. The system of claim 2, wherein the at least one processor is configured to:
encrypt each of the at least one set of encrypted asset encryption key parts using a public key of a public/private keypair associated with a corresponding part holder, such that each of the at least one set of encrypted asset encryption key parts is double encrypted, first using the at least one public key of the public/private keypair associated with the system, and second using the public key of the public/private keypair associated with the corresponding part holder.

4. The system of claim 3, further comprising:
a network adapter communicatively coupled to the at least one processor and configured to:
communicate each of the at least one set of encrypted asset encryption key parts to the corresponding part holder.
5. The system of claim 3, further comprising:
a network adapter communicatively coupled to the at least one processor and configured to:
communicate each of the at least one set of encrypted asset encryption key parts to a repository for later access by the corresponding part holder.
6. The system of claim 3, wherein each part holder is configured to:
decrypt a corresponding encrypted asset encryption key part using a private key of the public/private keypair associated with the corresponding part holder; and
re-encrypt the corresponding encrypted asset encryption key part, using the at least one public key of the at least one public/private keypair associated with the system, to produce a re-encrypted asset encryption key part;
wherein the re-encrypted asset encryption key part are communicated from the corresponding part holder to the system to reconstruct the asset encryption key.
7. The system of claim 1, wherein using at least one of the at least one symmetric key or the at least one public key of the at least one public/private keypair associated with the system includes:
using the at least one symmetric key when the system implements an offline signing service, wherein the at least one symmetric key is stored in the at least one memory in the system.
8. The system of claim 7, wherein the at least one processor is configured to:
encrypt each of the at least one set of encrypted asset encryption key parts using a public key of a public/private keypair associated with the offline signing service, such that each of the at least one set of encrypted asset encryption key parts is double encrypted, first using the at least one symmetric key, and second using the public key of the public/private keypair associated with the system.

9. The system of claim 8, wherein the at least one processor is configured to:
cause a printer connected to the system to print a quick response (QR) code for each of the at least one set of encrypted asset encryption key parts.
10. The system of claim 9, wherein at least one QR code of the QR code for each of the at least one set of encrypted asset encryption key parts is scanned by an imaging device coupled to the system as part of reconstructing the asset encryption key.
11. The system of claim 1, wherein the at least one processor is configured to:
generate the at least one set of asset encryption key parts from the asset encryption key through at least one of polynomial interpolation or Shamir secret sharing.
12. The system of claim 1, wherein the action comprises at least one of the following actions using the at least one asset key:
encrypting first data;
decrypting second data;
encrypting a first blockchain private key;
decrypting a second blockchain private key;
generating a transaction address; or
signing a transaction.
13. A system 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:
receive a plurality of encrypted asset encryption key parts from a plurality of corresponding part holders;
decrypt the plurality of encrypted asset encryption key parts into asset encryption key parts using at least one of:
at least one symmetric key; or
at least one private key of at least one public/private keypair associated with the system; and

reconstruct an asset encryption key from the asset encryption key parts, wherein the asset encryption key is reconstructed from a quantity of the asset encryption key parts that is a subset of a total number of asset encryption key parts previously created from the asset encryption key.

14. The system of claim 13, wherein using the at least one symmetric key or the at least one private key of the at least one public/private keypair associated with the system includes:

using the at least one private key of the at least one public/private keypair associated with the system, when the system implements an online signing service, during decryption of the plurality of encrypted asset encryption key parts into the asset encryption key parts,

wherein the at least one private key of the at least one public/private keypair associated with the system is stored in the at least one memory in the system.

15. The system of claim 14, further comprising:

a network adapter communicatively coupled to the at least one processor;

wherein the at least one processor is configured to receive the plurality of encrypted asset encryption key parts from the plurality of corresponding part holders via a network using the network adapter.

16. The system of claim 14, further comprising:

a network adapter communicatively coupled to the at least one processor;

wherein the at least one processor is configured to receive the plurality of encrypted asset encryption key parts from the plurality of corresponding part holders via a repository using the network adapter, wherein the plurality of encrypted asset encryption key parts were previously stored in the repository by the plurality of corresponding part holders.

17. The system of claim 13, wherein using the at least one symmetric key or the at least one private key of the at least one public/private keypair associated with the system includes:

using the at least one symmetric key, when the system implements an offline signing service, during decryption of the plurality of encrypted asset encryption key parts into the asset encryption key parts,

wherein the at least one symmetric key is stored in the at least one memory in the system.

18. The system of claim 17, further comprising:
an imaging device communicatively coupled to the at least one processor and configured to read a quick response (QR) code for each of the plurality of encrypted asset encryption key parts;
wherein the at least one processor is configured to receive the plurality of encrypted asset encryption key parts from the plurality of corresponding part holders by processing data from the QR code for each of the plurality of encrypted asset encryption key parts.
19. The system of claim 13, wherein the at least one processor is further configured to perform an action using the asset encryption key reconstructed from the quantity of the asset encryption key parts.
20. The system of claim 19, wherein the action comprises decrypting an asset key using the asset encryption key reconstructed from the quantity of the asset encryption key parts.
21. The system of claim 20, wherein the action comprises signing a transaction using the asset key decrypted using the asset encryption key.
22. A method for splitting an asset encryption key, the method being performed by a system, the method comprising:
splitting the asset encryption key into at least one set of asset encryption key parts;
and
encrypting the at least one set of asset encryption key parts into at least one set of encrypted asset encryption key parts using at least one of:
at least one symmetric key; or
at least one public key of at least one public/private keypair associated with the system;
wherein at least a subset of the at least one set of asset encryption key parts are used to reconstruct the asset encryption key, which is used to perform an action using at least one asset key.
23. The method of claim 22, wherein using at least one of the at least one symmetric key or the at least one public key of the at least one public/private keypair associated with the system includes:

using the at least one public key of the at least one public/private keypair associated with the system when the system implements an online signing service,

wherein at least one private key, corresponding to the at least one public key of the at least one public/private keypair associated with the system, is stored in at least one memory in the system.

24. The method of claim 23, further comprising:

encrypting each of the at least one set of encrypted asset encryption key parts using a public key of a public/private keypair associated with a corresponding part holder, such that each of the at least one set of encrypted asset encryption key parts is double encrypted, first using the at least one public key of the public/private keypair associated with the system, and second using the public key of the public/private keypair associated with the corresponding part holder.

25. The method of claim 24, further comprising:

communicating the at least one set of encrypted asset encryption key parts to corresponding part holders.

26. The method of claim 22, wherein using at least one of the at least one symmetric key or the at least one public key of the at least one public/private keypair associated with the system includes:

using the at least one symmetric key when the system implements an offline signing service, wherein the at least one symmetric key is stored in the system.

27. The method of claim 26, further comprising:

encrypting each of the at least one set of encrypted asset encryption key parts using a public key of a public/private keypair associated with the offline signing service, such that each of the at least one set of encrypted asset encryption key parts is double encrypted, first using the at least one symmetric key, and second using the public key of the public/private keypair associated with the system.

28. The method of claim 27, wherein each encrypted asset encryption key part is communicated to a respective part holder as a printout of a quick response (QR) code.

29. The method of claim 22, further comprising:
decrypting at least a second subset of the at least one set of encrypted asset encryption key parts to produce asset encryption key parts.
30. The method of claim 22, wherein the action comprises at least one of the following actions using the at least one asset key:
encrypting first data;
decrypting second data;
encrypting a first blockchain private key;
decrypting a second blockchain private key;
generating a transaction address; or
signing a transaction.