

CLAIMS

What is claimed is:

1. A method for blockchain-based secure storage, comprising:
in an information processing apparatus comprising at least one computer processor:
receiving a plurality of data files from a data file source;
bundling the plurality of data files into a package;
generating a first hash for each file name for each of the plurality of data files, and a second hash for contents of each of the plurality of data files;
generating a block comprising the first hash, the second hash, and a reference to a prior block;
encrypting each of the plurality of data files in the package;
sending the plurality of packages to a storage provider; and
committing the block to a distributed ledger.
2. The method of claim 1, wherein the data files are bundled based on a type of data in the data files.
3. The method of claim 1, wherein the data files are bundled based on a source of data in the data files.
4. The method of claim 1, wherein the data files are bundled based on an application associated with the data files.
5. The method of claim 1, wherein the data files are bundled based on a user associated with the data files.
6. The method of claim 1, further comprising:

selecting the storage provider from a plurality of storage providers.

7. The method of claim 1, further comprising:
combining metadata for a plurality of packages into a capsule; and
storing the capsule.

8. The method of claim 7, wherein the metadata comprises at least one of a capsule ID, a nonce, a hash of the block, a hash of the prior block, and a date and time of capsule creation.

9. The method of claim 7, wherein the metadata comprises a public key for the capsule.

10. The method of claim 9, wherein a private key corresponding the public key is provided to team members to access the metadata.

11. A system for blockchain-based secure storage, comprising:
a data file source;
a distributed ledger;
a storage provider; and
an information processing apparatus comprising at least one computer processor and executing a computer program;
wherein:

the computer program receives a plurality of data files from a system;

the computer program bundles the plurality of data files into a package;

the computer program generates a first hash for each file name for each of the plurality of data files, and a second hash for contents of each of the plurality of data files;

the computer program generates a block comprising the first hash, the second hash, and a reference to a prior block;

the computer program encrypts each of the plurality of data files in the package;

the computer program sends the plurality of packages to a storage provider; and

the computer program commits the block to a distributed ledger.

12. The system of claim 11, wherein the data files are bundled based on a type of data in the data files.

13. The system of claim 11, wherein the data files are bundled based on a source of data in the data files.

14. The system of claim 11, wherein the data files are bundled based on an application associated with the data files.

15. The system of claim 11, wherein the data files are bundled based on a user associated with the data files.

16. The system of claim 11, wherein the computer program further selects the storage provider from a plurality of storage providers.

17. The system of claim 11, wherein the computer program further combines metadata for a plurality of packages into a capsule, and stores the capsule.

18. The system of claim 17, wherein the metadata comprises at least one of a capsule ID, a nonce, a hash of the block, a hash of the prior block, and a date and time of capsule creation.

19. The system of claim 17, wherein the metadata comprises a public key for the capsule.

20. The system of claim 19, wherein a private key corresponding the public key is provided to team members to access the metadata.