

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, wherein the data files are bundled in the package based on a type of data in the data files and based on a user associated with the data files;
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~~package to a storage provider; ~~and~~
committing the block to a distributed ledger;
combining metadata for a plurality of packages, including the package, into a capsule wherein the metadata comprises a public key for the capsule, and a notification indication, and wherein the notification indication includes a notification preference of the user associated with the data files;
storing the capsule; and
providing a private key that corresponds to the public key to the user associated with the data files.
2. The method of claim 1, wherein the data files are bundled based on a ~~type~~source 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~~ 4. The method of claim 1, further comprising:
selecting the storage provider from a plurality of storage providers.

~~7~~ 5. 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~~ 6. 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 data file source;

the computer program bundles the plurality of data files into a package, and wherein the data files are bundled in the package based on a type of data in the data files and based on a user associated with the data files;

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~~package to ~~a~~the storage provider; ~~and~~

the computer program commits the block to ~~a~~the 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 computer program combines metadata for a plurality of packages, including the package, into a capsule wherein the metadata comprises a public key for the capsule, and a notification indication, and wherein the notification indication includes a notification preference of the user associated with the data files;

the computer program stores the capsule; and

the computer program provides a private key that corresponds to the public key to the user associated with the data files.

7. The system of claim ~~44~~6, wherein the data files are bundled based on a source of data in the data files.

~~48.~~ The system of claim ~~44~~6, wherein the data files are bundled based on an application associated with the data files.

~~49.~~ The system of claim ~~44~~, wherein the data files are bundled based on a user associated with the data files.

~~16.~~ The system of claim ~~44~~6, wherein the computer program further selects the storage provider from a plurality of storage providers.

~~17~~

10. The system of claim ~~44~~, wherein the computer program further combines metadata for a plurality of packages into a capsule, and stores the capsule.

~~18. The system of claim 176~~, 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.

~~1911. The method of claim 1, wherein the notification indication includes an electronic mail address of the user associated with the data files.~~

12. The method of claim 1, wherein the notification indication includes an indication that the user associated with the data files will receive a notification when a new block based on the package is added to the distributed ledger.

13. The system of claim 176, wherein the ~~metadata comprises a public key for~~notification indication includes an electronic mail address of the capsule user associated with the data files.

~~2014. The system of claim 196, wherein a private key corresponding the public key~~notification indication includes an indication that the user associated with the data files will receive a notification when a new block based on the package is provided~~added to team members to access the metadata.~~

the distributed ledger.