

CLAIMS

1. A computer-implemented method, comprising:
 - storing a data item in a consortium blockchain maintained by a consortium blockchain network;
 - generating a first data digest based on the stored data item;
 - sending a copy of the first data digest to each of a plurality of verification nodes participating in a public blockchain network so that each verification node cryptographically signs the first data digest and stores a corresponding copy of a first cryptographically signed first data digest in a public blockchain maintained by the public blockchain network;
 - receiving, by the consortium blockchain network, a request to retrieve the stored data item;
 - in response to receiving the request, retrieving the requested data item from the consortium blockchain;
 - generating a second data digest based on the retrieved data item from the consortium blockchain;
 - sending a copy of the second data digest to each of the plurality of verification nodes so that each verification node cryptographically signs the second data digest and returns a corresponding copy of a second cryptographically signed second data digest;
 - receiving the second cryptographically signed second data digests from the plurality of verification nodes;
 - retrieving the first cryptographically signed first data digests from the plurality of verification nodes of the public blockchain by identifying the first cryptographically signed first data digests based on an identifier associated with the stored data item and stored in the public blockchain;
 - determining that the first cryptographically signed first data digests match the second cryptographically signed second data digests; and
 - in response to determining that the first cryptographically signed first data digests match the second cryptographically signed second data digests, sending a response to the request to retrieve the stored data item, the response indicating that the stored data item has not changed since it was stored in the consortium blockchain.

2. The computer-implemented method of claim 1, further comprising storing a smart contract in the public blockchain, wherein the smart contract is configured to provide a monetary reward to the plurality of verification nodes in response to receiving the requested second cryptographically signed second data digests from the plurality of verification nodes.
3. The computer-implemented method of claim 1, wherein generating the first data digest includes calculating a hash of the stored data item.
4. The computer-implemented method of claim 1, wherein each verification node is configured to cryptographically sign the first data digest using a private key associated with that verification node.
5. The computer-implemented method of claim 1, wherein sending the first data digest to the plurality of verification nodes includes broadcasting the first data digest to the public blockchain network.
6. A non-transitory computer-readable storage medium storing one or more instructions executable by a computer system to perform operations comprising:
 - storing a data item in a consortium blockchain maintained by a consortium blockchain network;
 - generating a first data digest based on the stored data item;
 - sending a copy of the first data digest to each of a plurality of verification nodes participating in a public blockchain network so that each verification node cryptographically signs the first data digest and stores a corresponding copy of a first cryptographically signed first data digest in a public blockchain maintained by the public blockchain network;
 - receiving, by the consortium blockchain network, a request to retrieve the stored data item;
 - in response to receiving the request, retrieving the requested data item from the consortium blockchain;

generating a second data digest based on the retrieved data item from the consortium blockchain;

sending a copy of the second data digest to each of the plurality of verification nodes so that each verification node cryptographically signs the second data digest and returns a corresponding copy of a second cryptographically signed second data digest;

receiving the second cryptographically signed second data digests from the plurality of verification nodes;

retrieving the first cryptographically signed first data digests from the plurality of verification nodes of the public blockchain by identifying the first cryptographically signed first data digests based on an identifier associated with the stored data item and stored in the public blockchain;

determining that the first cryptographically signed first data digests match the second cryptographically signed second data digests; and

in response to determining that the first cryptographically signed first data digests match the second cryptographically signed second data digests, sending a response to the request to retrieve the stored data item, the response indicating that the stored data item has not changed since it was stored in the consortium blockchain.

7. The non-transitory computer-readable storage medium of claim 6, wherein the operations comprise:

store a smart contract in the public blockchain, wherein the smart contract is configured to provide a monetary reward to the plurality of verification nodes in response to receiving the requested second cryptographically signed second data digests from the plurality of verification nodes.

8. The non-transitory computer-readable storage medium of claim 6, wherein generating the first data digest includes calculating a hash of the stored data item.

9. The non-transitory computer-readable storage medium of claim 6, wherein each verification node is configured to cryptographically sign the first data digest using a private key associated with that verification node.

10. The non-transitory computer-readable storage medium of claim 6, wherein sending the first data digest to the plurality of verification nodes includes broadcasting the first data digest to the public blockchain network.

11. A system, comprising:

one or more computers; and

one or more computer memory devices interoperably coupled with the one or more computers and having tangible, non-transitory, machine-readable media storing one or more instructions that, when executed by the one or more computers, perform one or more operations comprising:

storing a data item in a consortium blockchain maintained by a consortium blockchain network;

generating a first data digest based on the stored data item;

sending a copy of the first data digest to each of a plurality of verification nodes participating in a public blockchain network so that each verification node cryptographically signs the first data digest and stores a corresponding copy of a first cryptographically signed first data digest in a public blockchain maintained by the public blockchain network;

receiving, by the consortium blockchain network, a request to retrieve the stored data item;

in response to receiving the request, retrieving the requested data item from the consortium blockchain;

generating a second data digest based on the retrieved data item from the consortium blockchain;

sending a copy of the second data digest to each of the plurality of verification nodes so that each verification node cryptographically signs the second data digest and returns a corresponding copy of a second cryptographically signed second data digest;

receiving the second cryptographically signed second data digests from the plurality of verification nodes;

retrieving the first cryptographically signed first data digests from the plurality of verification nodes of the public blockchain by identifying the first cryptographically signed first data digests based on an identifier associated with the stored data item and stored in the public blockchain;

determining that the first cryptographically signed first data digests match the second cryptographically signed second data digests; and

in response to determining that the first cryptographically signed first data digests match the second cryptographically signed second data digests, sending a response to the request to retrieve the stored data item, the response indicating that the stored data item has not changed since it was stored in the consortium blockchain.

12. The system of claim 11, wherein the operations further comprise:

store a smart contract in the public blockchain, wherein the smart contract is configured to provide a monetary reward to the plurality of verification nodes in response to receiving the requested second cryptographically signed second data digests from the plurality of verification nodes.

13. The system of claim 11, wherein generating the first data digest includes calculating a hash of the stored data item.

14. The system of claim 11, wherein each verification node is configured to cryptographically sign the first data digest using a private key associated with that verification node.

15. The system of claim 11, wherein sending the first data digest to the plurality of verification nodes includes broadcasting the first data digest to the public blockchain network.