

WHAT IS CLAIMED IS:

1. A computer-implemented method for protecting sensitive data stored on a blockchain maintained by a blockchain network, the method comprising:

5 receiving, by a blockchain node in the blockchain network, a request to read a particular block of the blockchain, wherein the request is received from a light-weight node of the blockchain network and includes an identity of the light-weight node, and wherein the particular block includes an original Merkle tree containing a plurality of transactions associated with the particular block;

10 identifying, by the blockchain node, permissions associated with the identity of the light-weight node;

generating, by the blockchain node, an isolated Merkle tree based on the original Merkle tree included in the particular block, the isolated Merkle tree including only transactions from the original Merkle tree that are determined to be accessible by the light-weight node based on the identified permissions, wherein the isolated Merkle tree is consistent with the original Merkle tree; and

15 sending, by the blockchain node, a response to the light-weight node including the isolated Merkle tree.

20 2. The computer-implemented method of claim 1, wherein generating the isolated Merkle tree based on the original Merkle tree included in the particular block includes:

modifying the original Merkle tree to produce the isolated Merkle tree, including:

removing all transactions that are determined to not be accessible by the light-weight node from the original Merkle tree; and

25 removing branches of the original Merkle tree from which all transactions have been removed leaving only the root hash of each of the branches intact.

3. The computer-implemented method of claim 2, wherein a transaction is determined to not to be accessible by the light-weight node if the permissions indicate that the light-weight node does not have read access to the transaction.

30

4. The computer-implemented method of claim 1, wherein each of the plurality of transactions includes one or more identities associated with one or more participants in the transaction.
- 5 5. The computer-implemented method of claim 4, wherein the identity is associated with an identity class, the permissions are associated with the identity class, and the blockchain node is configured to enforce permissions associated with the identity class on identities associated with the identity class.
- 10 6. The computer-implemented method of claim 5, wherein the identity class is a regulator class, and wherein the permissions associated with the regulator class indicate that all transactions in the blockchain network are accessible to identities associated with the regulator class.
- 15 7. The computer-implemented method of claim 5, wherein the identity class is a common class, and wherein the permissions associated with the common class indicate that only transactions in the blockchain network in which the identity is a participant are accessible to the identity.
- 20 8. The computer-implemented method of claim 1, wherein the isolated Merkle tree is consistent with the original Merkle tree only if it is sufficient to enable the light-weight node to verify integrity of the block based on the isolated Merkle tree.
- 25 9. A non-transitory computer-readable storage medium coupled to one or more processors and having instructions stored thereon which, when executed by the one or more processors, cause the one or more processors to perform operations in accordance with the method of one or more of claims 1-8.
- 30 10. A system, comprising:
a computing device; and

a computer-readable storage device coupled to the computing device and having instructions stored thereon which, when executed by the computing device, cause the computing device to perform operations in accordance with the method of one or more of claims 1-8.