

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, wherein the particular block includes an original Merkle tree containing a plurality of transactions associated with the particular block, and wherein each transaction of the
10 plurality of transactions includes one or more identities associated with one or more participants in the transaction;

identifying, by the blockchain node, based on permissions associated with the identity of the light-weight node, that the light-weight node has access to transactions in which the light-weight node is a participant;

15 generating, by the blockchain node, an isolated Merkle tree based on the original Merkle tree included in the particular block, comprising:

removing, from the original Merkle tree, transactions in which the light-weight node is not a participant, and

removing branches of the original Merkle tree from which all transactions
20 have been removed, leaving a root hash of each removed branch intact, wherein the isolated Merkle tree is usable by the light-weight node to verify integrity of the isolated Merkle tree based on root hashes included in the isolated Merkle tree;
and

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

2. The computer-implemented method of claim 1, wherein generating the isolated Merkle tree comprises:

i) starting from a first transaction of the plurality of transactions, sequentially
30 scanning transactions and determining, for each scanned transaction, whether the light-weight node is a participant in the scanned transaction,

ii) in response to scanning a second transaction, after the first transaction, in which the light-weight node is not a participant, continuing to scan transactions and determine, for each scanned transaction, whether the light-weight node is a participant in the scanned transaction,

5 iii) in response to scanning a third transaction, after the second transaction, that is an earliest-scanned transaction after the second transaction in which the light-weight node is a participant, removing a group of transactions including the second transaction and all transactions between the second transaction and the third transaction,

 iv) removing, from the original Merkle tree, branches from which all transactions
10 have been removed, and

 repeating steps i)-iv) until a last transaction in the original Merkle tree has been scanned.

3. The computer-implemented method of claim 1, wherein each transaction of the
15 plurality of transactions is determined to not to be accessible by the light-weight node if the permissions associated with the identity of the light-weight node indicate that the light-weight node does not have read access to the transaction.

4. The computer-implemented method of claim 1, wherein the identity of the light-
20 weight node is associated with an identity class, the permissions associated with the identity of the light-weight node 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.

25 5. The computer-implemented method of claim 4, wherein a first identity class is a regulator class, and wherein permissions associated with the regulator class indicate that all transactions in the blockchain network are accessible to identities associated with the regulator class.

30 6. The computer-implemented method of claim 4, wherein the identity class associated with the identity of the light-weight node is a common class.

7. A non-transitory computer-readable storage medium coupled to one or more
5 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 1-6.

8. A system, comprising:

10 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 1-6.