

What is claimed is:

1. A computer-implemented method of block propagation in a blockchain network, comprising:
 - constructing, at a first mining node, a first candidate block containing transactions in a first ordered set, the first candidate block having a first block header;
 - placing one or more invalid transactions in the first ordered set to create a poisoned ordered set;
 - constructing a list identifying the one or more invalid transactions within the poisoned ordered set, and encrypting the list to produce an encrypted list of invalid transactions; and
 - while hashing the first block header, sending, to other mining nodes, a first message containing the poisoned ordered set and the encrypted list of invalid transactions.
2. The method of claim 1, further comprising the first mining node finding a proof-of-work with respect to the first block header and, as a result, sending a decryption key for the encrypted list of invalid transactions.
3. The method of claim 1 or claim 2, wherein placing one or more invalid transactions includes inserting the one or more invalid transactions into the first ordered set of transactions.
4. The method of claim 1 or claim 2, wherein placing one or more invalid transactions includes, for each invalid transaction in the one or more invalid transactions, replacing a respective valid transaction in the first ordered set.
5. The method of claim 4, wherein the encrypted list of invalid transactions further includes the respective valid transactions.

6. The method of claim 4 or claim 5, further comprising, at another mining node, constructing the first candidate block by decrypting the encrypted list of invalid transactions, replacing the one or more invalid transactions with the respective valid transactions in the poisoned ordered set in order to reconstruct the first ordered set and generate the first candidate block.
7. The method of any one of claims 1 to 6, wherein the one or more invalid transactions includes a transaction that violates at least one validity criteria prescribed by a blockchain protocol for the blockchain network.
8. The method of any one of claims 1 to 7, further comprising, at the first mining node, creating at least one of the one or more invalid transactions.
9. The method of any one of claims 1 to 8, further comprising, at the first mining node, selecting as one of the one or more invalid transactions an invalid transaction received from another mining node.
10. The method of claim 1, further comprising the first mining node finding a proof-of-work with respect to the first block header and, as a result, sending the proof-of-work and a decryption key for the encrypted list of invalid transactions, wherein the proof-of-work includes a coinbase transaction from the first candidate block, and a nonce and timestamp from the first block header.
11. The method of claim 1, further comprising, while hashing the first block header, receiving a second message identifying transactions and their order in a second poisoned ordered set derived from a second candidate block being mined by a second mining node, and receiving a second encrypted list, wherein the second encrypted list identifies invalid transactions within the second poisoned ordered set.

12. The method of claim 11, further comprising validating the transactions in the second poisoned ordered set and identifying a set of one or more invalid transactions in the second poisoned ordered set.
13. The method of claim 12, further comprising:
 - receiving a coinbase transaction, a decryption key, and second block header information from the second mining node indicating successful completion of a proof-of-work with regard to the second candidate block, wherein the second block header information includes at least a timestamp and a nonce;
 - decrypting the second encrypted list using the decryption key;
 - determining that the second encrypted list identifies the same invalid transactions as in the set of one or more invalid transactions;
 - assembling a second block header based on the coinbase transaction, the second block header information, and the second poisoned ordered set modified to replace the one or more invalid transactions in the second poisoned ordered set; and
 - validating the second candidate block by hashing the second block header to validate the proof-of-work.
14. A computing device implementing a first mining node for mining blocks on a blockchain network, the computing device including:
 - one or more processors;
 - memory;
 - computer-executable instructions stored in the memory that, when executed by the one or more processors, cause the processors to carry out the method claimed in any one of claims 1 to 13.
15. A computer-readable medium storing processor-executable instructions for implementing a first mining node for mining blocks on a blockchain network, the processor-executable

instructions including instructions that, when executed by one or more processors, cause the processors to carry out the method claimed in any one of claims 1 to 13.