

CLAIMS

WHAT IS CLAIMED IS:

1. A computer-implemented method for enhancing blockchain network security, comprising:

5 receiving, by a blockchain node, a transaction request from a client during a communication session between the blockchain node and the client, wherein the transaction request includes a transaction requested to be recorded on a blockchain and a transaction hash calculated by hashing the transaction with a pseudo-random value generated for the blockchain node and a password that is unique to the client and input by
10 the client during the communication session;

determining, by the blockchain node, the transaction hash is not previously stored in a cache resource or the blockchain;

storing the transaction hash in the cache resource; and

executing the transaction request.

15 2. The computer-implemented method of claim 1, wherein the transaction request includes a digital signature generated based on the transaction, wherein the digital signature comprises an asymmetric encryption of the transaction hash.

20 3. The computer-implemented method of any one of the preceding claims, wherein determining the transaction hash is not previously stored in the cache resource or the blockchain includes:

querying the cache resource using the transaction hash; and

25 determining that an identical copy of the transaction hash is not stored in the cache resource.

4. The computer-implemented method of claim 3, wherein the cache resource implements a bloom filter that stores transaction hashes received by the blockchain node prior to receiving the transaction request.

5. The computer-implemented method of claim 4, wherein the transaction is a first transaction and the transaction hash is a first transaction hash, the method further comprising:

5 receiving, by the blockchain node, a second transaction request including a second transaction and a second transaction hash;

determining, by the blockchain node, the second transaction hash is previously stored in at least one of the cache resource and the blockchain, the previous storage of the second transaction hash in the at least one of the cache resource and the blockchain
10 indicating a network attack in which an attacker intercepted the first transaction request; and

sending, by the blockchain node, a transaction rejection in response to the second transaction request to the client to counter the network attack.

15 6. The computer-implemented method of any one of claims 1-3, wherein the transaction is a first transaction and the transaction hash is a first transaction hash, and the method further comprising:

receiving, by the blockchain node, a second transaction request including a second transaction and a second transaction hash;

20 determining, by the blockchain node, the second transaction hash is previously stored in the blockchain, the previous storage of the second transaction hash in the blockchain indicating a network attack in which an attacker intercepted the first transaction request; and

25 sending, by the blockchain node, a transaction rejection in response to the second transaction request to the client to counter the network attack.

7. The computer-implemented method of any one of the preceding claims, wherein the transaction includes information associated with one or more of a blockchain address, a transaction amount, and a time of the transaction.

8. A system for enhancing blockchain network security, comprising:

one or more processors; and

one or more computer-readable memories coupled to the one or more processors

5 and having instructions stored thereon that are executable by the one or more processors
to perform the method of any of claims 1 to 7.

9. An apparatus for enhancing blockchain network security, the apparatus
comprising a plurality of modules for performing the method of any of claims 1 to 7.

10