

What is claimed is:

1. A computer-implemented method of recording work history of a mining node on a blockchain in a blockchain network, comprising:
 - mining, by the mining node, a first block containing a registration generation transaction having an output that includes, within a registration information field, a miner identifier for the mining node; and
 - mining, by the mining node, two or more additional blocks in an order, each additional block containing a respective generation transaction each of which includes an output having an information field containing the miner identifier, a reference to the generation transaction of the preceding additional block in the order, wherein the registration generation transaction is a first block in the order.
2. The method claimed in claim 1, wherein the miner identifier is a public key for which the mining node holds a private key.
3. The method claimed in claim 1 or claim 2, wherein the generation transaction in each of the additional blocks includes a registration reference pointing to the registration generation transaction and a digital signature.
4. The method claimed in any one of claims 1 to 3, wherein the reference to the generation transaction of the preceding additional block in the order includes one of a transaction identifier, a block number, or an outpoint.
5. The method claimed in any one of claims 1 to 4, further comprising verifying, by a computing node, the work history recorded on the blockchain, wherein the verifying includes:
 - identifying a last block in the order;

retrieving, from the blockchain, the generation transactions from the additional blocks, in a reverse order, based on the reference to the generation transaction of the preceding additional block contained in each of the generation transactions;

retrieving the registration generation transaction; and

verifying the registration of the miner identifier in the registration generation transaction,

whereby the registration generation transaction and the generation transactions provide the work history of the mining node.

6. The method claimed in any one of claims 1 to 5, further comprising determining a reputation score for the mining node based on its recorded work history, wherein determining includes calculating the reputation score based on count of a number of blocks in the order.
7. The method claimed in any one of claims 1 to 5, further comprising determining a reputation score for the mining node based on its recorded work history, wherein determining includes calculating the reputation score based on:
 - assigning a respective weight to each block in the order; and
 - calculating a sum of the respective weights.
8. The method claimed in claim 7, wherein assigning a respective weight to each block includes, for each block, determining a difficulty score for that block based on a difficulty threshold applied in mining that block and setting the respective weight based on the difficulty score.
9. The method claimed in claim 7 or claim 8, wherein the reputation score is calculated as:

$$Rep_{ID} = f(T_i) = \sum_i^B 2^{256}/T_i$$

wherein Rep_{ID} is the reputation score, i is an index referring to the i th block, B is the number of blocks in the order, and T_i is a target difficulty applied in mining block i .

10. The method claimed in any one of claims 6 to 9, further comprising recording a weighted vote in a secure blockchain-based voting system by mining, by the mining node, a vote block, wherein the vote block contains a generation transaction that contains its miner identifier, a reference to its most recent generation transaction, and a vote signal.
11. The method claimed in claim 10, wherein the vote block generation transaction further includes the calculated reputation score for the mining node.
12. A computer-implemented method of verifying a work history of a mining node on a blockchain in a blockchain network, comprising:
 - identifying a block mined by the mining node and having a generation transaction having an output that includes, in an information field, a miner identifier, and a reference to an earlier generation transaction;
 - retrieving, from the blockchain, a plurality of earlier generation transactions, in a reverse order, each of which contains, in an output to each respective generation transaction, the miner identifier and a reference to a respective preceding one of the earlier generation transactions in the reverse order, until an earliest generation transaction that includes a registration with regard to the miner identifier; and
 - verifying the registration of the miner identifier in the earliest generation transaction,
 whereby the generation transaction and the plurality of earlier generation transactions provide the work history of the mining node.

13. A computer-implemented method of determining a reputation score for a mining node in a blockchain network based on a blockchain, comprising:
 - tracing a chain of linked generation transactions, wherein the generation transactions each include, in an output containing an information field, a miner identifier for the mining node, and each of which, excluding a first generation transaction, includes in the information field a reference to an earlier one of linked generation transactions in the chain, wherein each generation transaction is in a respective block mined by the mining node;
 - for each of the generation transactions, determining a difficulty score of its respective block; and
 - determining the reputation score for the mining node based the difficulty scores of respective blocks associated with the generation transactions in the chain.
14. A computing device to manage a public key infrastructure using a blockchain network, the computing device including:
 - one or more processors;
 - memory; and
 - 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 managing a public key infrastructure using 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.