What is claimed is:

1. A computer-implemented method of registering identity of a mining node on a blockchain in a blockchain network, comprising:

creating a validity-check transaction having a first output controlled by the mining node, and a second output providing an information field containing a miner identifier;

propagating the validity-check transaction on the blockchain network; and

mining, by the mining node, a new block containing a generation transaction, wherein the generation transaction includes, as an output, another information field that contains the miner identifier, wherein the information field of the generation transaction also contains a reference to the validity-check transaction,

whereby another node is enabled to verify validity of the miner identifier through receiving the miner identity, retrieving a copy of the generation transaction from the blockchain, retrieving a copy of the validity-check transaction from the blockchain based on the reference contained in the generation transaction, confirming that the received miner identifier matches the miner identifier contained in the generation transaction and in the validity-check transaction, and determining whether the miner identifier is valid through determining whether the first output of the validity-check transaction is within an unspent transaction output set for the blockchain network;

wherein the miner identifier is invalidated when the miner spends the first output, thereby removing it from the unspent transaction output set for the blockchain network.

2. The method of claim 1, wherein the miner identifier comprises a first public key for which the mining node holds a corresponding private key.

3. The method of claim 2, wherein the first public key is in the information field of the second output of the validity check transaction.

4. The method of claim 3, wherein the second output uses an OP_RETURN code.

5. The method of any one of claims 1 to 4, wherein the output in the generation transaction includes an OP_RETURN output providing the information field of the generation transaction that contains both the miner identifier and the reference to the validity-check transaction.

6. The method of any one of claims 1 to 5, wherein the reference to the validity-check transaction includes a transaction identifier.

7. The method of any one of claims 1 to 6, wherein the information field of the generation transaction further includes one or more of an action identifier or a digital signature, wherein the digital signature is generated using a private key corresponding to the miner identifier.

8. The method of any one of claims 1 to 7, further comprising verifying, by a second node, the validity of the miner identifier by:

receiving the miner identifier;

retrieving a copy of the generation transaction from the blockchain;

retrieving a copy of the validity-check transaction from the blockchain based on the reference contained in the generation transaction;

confirming that the received miner identifier matches the miner identifier in the generation transaction and the miner identifier in the validity-check transaction; and

determining that the first output is within the unspent transaction output set for the blockchain network.

9. The method claimed in claim 8, wherein confirming further includes confirming that an action identifier in the generation transaction indicates registration.

10. The method claimed in claim 8 or claim 9, wherein confirming further includes validating a digital signature within the generation transaction based on the miner identifier.

11. The method claimed in any one of claims 1 to 7, further comprising revoking the miner identifier by:

creating a revocation transaction having the first output of the validity-check transaction as an input;

digitally signing the revocation transaction; and

propagating the revocation transaction on the blockchain network.

12. The method claimed in any one of claims 1 to 7, further comprising updating the miner identifier to register a new miner identifier by:

creating a new validity-check transaction having a new first output controlled by the mining node and containing the new miner identifier;

propagating the new validity-check transaction on the blockchain network; and

mining, by the mining node, a new block containing a new generation transaction, wherein the new generation transaction includes, as an output, a further information field that contains the miner identifier, the new miner identifier, a new reference to the new validity-check transaction, and a first digital signature based on the miner identifier and a second digital signature based on the new miner identifier.

13. The method claimed in claim 12, further comprising revoking the miner identifier by creating and propagating a transaction that includes the first output of the validity-check transaction as an input.

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.