Bitcoin Mining

James Donnel, Francis Fasola, Spencer Esclante, Trevor Silva
Computer Science
Rowan University

Bitcoin mining is the process of record keeping for Bitcoin.

As transactions are created by users spending Bitcoins, the transactions are grouped together in blocks which are then verified by miners. When a block is mined it is added to the top of the block chain and broadcast across the Bitcoin network, creating a secure record of transactions.

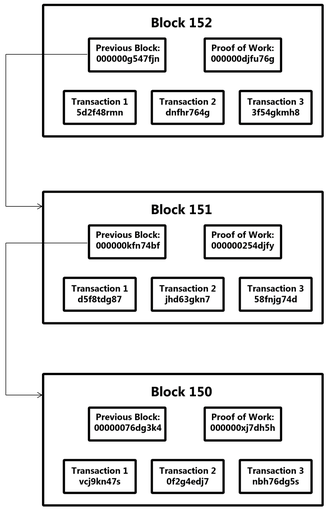

Figure 1. Block chain diagram

The block chain has a record of every block mined on the network.

The first block was mined on January 3, 2009; with each block coming after it referencing the previous block. Today the block chain has approximately 462,000 blocks with a new block mined around every ten minutes.

Miners are searching for a nonce.

A nonce is a number that when hashed with the contents of the block, it will be numerically smaller than Bitcoin network difficulty target. When a miner finds this nonce they broadcast their success to connected nodes on the network so the nodes can test the block was successfully mined. If the nodes approve of the new block they add the block to their chain and pass it to nodes they are connected to until it has reached the entire network of nodes.

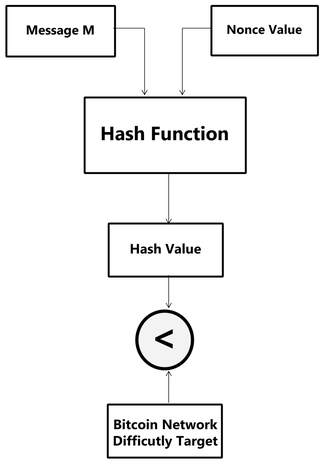

Figure 2. Mining Diagram.

Mining involves breaking a hash function.

Hash functions are used to map data of any size to a fixed size and produce a hash value for which only the input data can map to. A strong hash function maps similar data to very different hash values and uniformly distributes data across the entire set of possible values.

Miners can work together in a mining pool.

A mining pool is a group of miners who work together to mine the block and share the reward based on the amount of work contributed. Pools can contain thousands of miners working in parallel to mine the block.

Figure 3. Mining pool working to mine a new block.

Successfully mining a block rewards Bitcoins.

Each transaction has a transaction fee associated with it. When a block is mined, the miner is awarded all of the transaction fees along with a set number of Bitcoins. The number of Bitcoins rewarded decreases over time and around 2140 mining new blocks will not award new Bitcoins.

Acknowledgments

This project was sponsored by Professor Seth D. Bergman of the Rowan University Computer Science Department.