[PDF Database Document] - BTCC Cryptocurrency Exchange

Original:
https://www.btcc.com/en-US/academy/crypto-basics/how-bitcoin-mining-works

How Bitcoin Mining Works?

Bitcoins are discovered, not printed. Computers around the world compete with each other to "mine" the coins. This article will explain how bitcoin mining works.

Key Points:

- Bitcoin mining is the process of discovering new blocks, validating transactions, and adding them to the Bitcoin blockchain.
- Each time a new block is discovered, the successful miner has the right to populate the block with new transaction data.
- In return for investing time and resources to perform this task, the winning miner receives a free amount of newly minted Bitcoins, called a "block reward", as well as any fees associated with the transactions they store in the new block.
- The process of providing newly minted Bitcoins to successful miners is exactly how new coins are put into circulation.

Two Reasons for Bitcoin Mining

There are two primary reasons why a person, or company, would want to mine cryptocurrency like bitcoin.

1.To stand a chance of earning bitcoin block rewards (which, as of 2022, equals 6.25 bitcoins –approximately $210,000, at press time.) New blocks are roughly discovered once every 10 minutes.

2.To participate in securing and maintaining the decentralized Bitcoin network.

How New Blocks Are Discovered by Bitcoin Miners?

In order to validate and add new transactions to the blockchain, miners must compete with each other using specialized computing equipment. They use their equipment to generate fixed-length codes known as “hashes” (see below.) In order to discover the next block, miners must generate a hash that has an equal or higher number of zeros in front of it than the “target hash.”

The target hash is a 64-digit hexadecimal code (comprising numbers 0-9 and letters A-F) all miners are trying to get below in order to discover the next block.

As a starting point, all miners take the data from the previous block, known as the “block header”– which contains things like a timestamp of the block, the hash of the previous block data, and an empty space known as a “cryptographic nonce.” Most of the data in the block header is fixed, meaning it cannot be changed, apart from the nonce. A nonce means “a number only used once” and is the part of the previous block header that miners are allowed to tweak. Remember, just changing a single bit of the input produces a totally different hash.

The tricky part is, hashes are generated completely at random, meaning it’s impossible for miners to know what the hashes will be before they generate them. So it’s simply a case of trial and error until someone finds the right nonce value – known as the “golden nonce.”

This is why miners have to invest in energy-intensive computers, particularly application-specific integrated circuit (ASIC) miners, that can generate trillions of hashes per second.

An easy way to think of bitcoin mining is to imagine each new block is a treasure chest with a combination lock on it. To get the free bitcoin block reward inside and win the right to add new transaction data into it (and collect the associated fees) you have to keep turning one of the number wheels on the lock (the nonce) until you crack the combination (the target hash.)

Here’s an example of what a target hash might look like:

00000000000000000057fcc708cf0130d95e27c5819203e9f967ac56e4df598ee

To see just how difficult it is to generate a hash with more zeros at the front than the above target hash, try creating a winning hash yourself with this free online hash generator. Simply type anything you want in the text box provided and see if it produces a hash with more than 17 zeros at the front!

What Exactly Is a Hash?

A hash is a cryptographic mathematical function that converts any message or data input into a fixed-length code. Think of it as an encryption technique where messages are mathematically transposed into a sequence of numbers and letters of a fixed length.

The outputs have set lengths to make it impossible to guess the size of the input. For instance, the hash for the word “hi” would be exactly the same length as the hash of the entire text of a Harry Potter book.

These hash functions are irreversible, meaning that it’s impossible to revert the hash back to its original input. The same input will also always generate the same sequence of letters and numbers. For example, the hash of “hi” will be the same code every time. Each code generated is completely unique too, meaning it’s impossible to produce the same hash with two different inputs.

In the case of Bitcoin, the blockchain uses Secure Hash Algorithm 256 or SHA 256 to generate a 256 bit or 64 characters long output, regardless of the size of the input.

How Profitable Is Bitcoin Mining?

For every new block added to the blockchain, the protocol – a set of rules programmed into Bitcoin – releases a fixed amount of newly minted coins to the successful miner. This block reward system doubles as the distribution mechanism for Bitcoin.

As part of the programmed measures introduced by Satoshi Nakamoto to steadily decrease the number of bitcoins released over time, the coins awarded to miners are slashed roughly every four years, or 210,000 blocks, in a process known as a “Bitcoin Halving.” In 2009, the block reward was 50 BTC. This figure was reduced to 25 BTC in 2013. The most recent halving occurred in 2020, and saw block rewards fall from 12.5 BTC to 6.25 BTC.

Note that bitcoin has a 21 million maximum supply cap, and we already have 18.9 million coins in circulation. Block rewards will no longer be distributed once 21 million BTC has been released to the market. Once this happens, miners will only be able to earn rewards in the form of bitcoin transaction fees.

Even with this combination of two revenue sources, not every miner generates profits. To make ends meet, a miner’s earnings must exceed the amount spent on electricity and the purchase and maintenance of mining rigs. Also, as mining difficulty increases, large mining operations are forced to expand or upgrade their equipment to maintain a competitive edge. For most average miners who

cannot afford to invest in expensive equipment, there's an opportunity to combine their resources with other miners around the world. Each miner agrees to share rewards according to the contributions of each miner. These networks of miners are called "mining pools."

There are, however, some rare instances where solo miners have successfully mined blocks on their own from home.

Difficulty of Bitcoin Mining

An important thing to know about Bitcoin is that when Satoshi Nakamoto created the protocol, they programmed in a target block discovery time of 10 minutes. This means it should take approximately 10 minutes for a miner to successfully create the winning code to discover the next block.

So how does the network ensure new blocks are discovered every 10 minutes?

The Bitcoin protocol has the ability to automatically increase or decrease the complexity of the mining process depending on how quickly or slowly blocks are being found.

Every two weeks, the Bitcoin protocol automatically adjusts the target hash to make it harder or easier for miners to find blocks. If they are taking too long (more than 10 minutes) the difficulty will adjust downward; less than 10 minutes, it will adjust upward. More specifically, the protocol will increase or decrease the number of zeros at the front. This might not sound like much, but just adding a single zero to the target hash makes the code significantly harder to beat, and vice versa.

The 2021 crackdown on mining activities in China caused bitcoin's network difficulty to experience its biggest drop in history. This subsequently led to remaining bitcoin miners reporting significant rises in mining revenue.

Through this system, the Bitcoin protocol is able to keep block discovery times as close to 10 minutes as it can.

While actively participating in the Bitcoin network can be a highly rewarding venture, the electricity and hardware requirements often limit its profitability – particularly for miners with limited resources.

Why Does Bitcoin Mining Consume So Much Energy?

One of the biggest drawbacks of Bitcoin is the vast amount of energy it uses to mine new coins, validate transactions and secure its network. At press time, Bitcoin's hash rate – the measure of all computational power dedicated to mining new coins – stands at 183 exahash (Eh/s.) This means bitcoin miners collectively attempt to crack the target hash of the next new block 183 quintillion times per second.

According to the Cambridge Bitcoin Electricity Consumption Index (CBECI,) this activity consumes approximately 131 TeraWatt hours (TWh) of electricity per year – which is more electricity than the country of Ukraine consumes during the same time period.

The main reason for this extreme consumption is because each time bitcoin rises in price, it encourages new miners to join in the battle to win new coins and forces existing outfits to purchase more rigs or upgrade their equipment to remain competitive. When this happens, the amount of computational power used to mine bitcoin increases (hash rate increases) which, in turn, causes the bitcoin protocol to ramp up the difficulty so that blocks continue to be discovered at a steady rate every 10 minutes.

A natural byproduct of this increased competition is higher energy consumption – the more machines that start mining bitcoin, the higher the collective energy consumption.