

How Does Bitcoin Mining Work?

Original:

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

This article gives an explanation of the process of bitcoin mining, the requirements of becoming a bitcoin miner, whether it is profitable and more. Read now!

Bitcoin remains one of the most secure blockchains out there due to its specific consensus mechanism (known as <u>proof-of-work</u> (PoW)), and participation by a large network of miners. In addition to the security provided by <u>mining</u>, the process also functions as the sole issuance system for the cryptocurrency: newly minted coins are released to miners as incentives.

Bitcoin's high levels of security, popularity and value as an asset mean that mining its blockchain has retained its appeal, notwithstanding the fact that the number of coins awarded to miners is slashed – by design – roughly every four years (this is known as halving).

And so you may ask: how exactly do Bitcoin miners capitalize on the infrastructural design of the Bitcoin network to generate profits? This article aims to provide a brief overview of the processes behind the market's most popular cryptocurrency. It also gives some insights into what it can take to become a potentially profitable Bitcoin miner yourself.

What Exactly Is Bitcoin Mining?

Bitcoin mining is a critical component for the security of the Bitcoin network, as well as being the sole mechanism for the issuance of new coins. Those involved in this operation, known as miners, mobilize powerful computing equipment to compete to become successful validators of new blocks on the Bitcoin blockchain – and thereby to pocket both network transaction fees and newly minted coins.

While this brief explanation summarizes the overall role and nature of Bitcoin mining, it does not clarify its technical aspects. The following will provide a more in-depth guide to the operations of Bitcoin miners.



How Does Bitcoin Mining Operate?

Miners function as auditors of the Bitcoin network as their role is to verify the validity of new transactions and, once verified, to add them to the blockchain.

Importantly, this task helps eliminate the possibility of what is known as double spending. Unlike the fiat currency system, the decentralized structure of cryptocurrency networks exposes them to this unique type of problem. For the network to be viable, it must be possible to verify that participants are not trying to outsmart the system by spending the same coin twice — and this must be done without the intervention of banks or any other intermediary.

Recall that in the case of fiat currencies, a person either spends a physical bill or coin – and therefore no longer has it in their possession – or else a bank audits their transactions and continually updates the balance on their accounts.

To prevent the possibility of double spending, miners are tasked with verifying transactions. At each instance, miners confirm the validity of 1 MB worth of new Bitcoin transactions, which are then added to the Bitcoin blockchain so long as they successfully fulfill other requirements imposed by the network's consensus mechanism. You may be wondering: why are they restricted to 1 MB of transactions? Well, the answer lies in the infrastructural design of the Bitcoin protocol.

Note that Bitcoin's underlying technology is blockchain, which, as its name implies, involves a sequential chain of blocks containing records of past transactions. Bitcoin's creator designed each block to have a fixed 1 MB size. It is therefore impossible to load transaction data that exceeds this limit.

After verifying 1 MB worth of transactions, the miner becomes eligible to mine new coins. That said, this does not mean that the miner will automatically be awarded Bitcoins as a reward for verifying

these transactions. Instead, the miner must compete with other miners to become *the first on the network* to successfully verify and therefore underwrite the next new block of transactions on the Bitcoin blockchain. This is where all the fun begins.

Can Bitcoin Miners Solve Complex Mathematical Puzzles?

Bitcoin miners indeed have to set up and operate powerful and sophisticated computing equipment that can attempt to solve highly complex mathematical problems. This is the core requirement for becoming a successful Bitcoin miner. The profitability of miners' operations relies heavily upon the quality of their hardware and how quickly it is able to solve these problems ahead of other, competing miners.

This is where it's useful to know something about Bitcoin's particular design and consensus algorithm. For its security, the network's proof-of-work system uses what is known in cryptography as a Secure Hashing Algorithm-256 (SHA-256) hash function. SHA-256 outputs 256 bits long hash values as outputs in order to encrypt inputs (in this case, Bitcoin transactions), hence the name.

These hashes are pseudorandom and it is therefore almost impossible to predict the output of any input before actually running the input through the hash function. In order to add a new block to the blockchain and claim their reward of newly mined Bitcoin, miners therefore use their computing resources to engage in an intensive and extremely fast form of mathematical guesswork, with the aim of producing a valid hash value that is below a certain threshold, known as the target.

The odds of guessing the right target are extremely low. Notably, these odds become tougher still in tandem with the competitiveness of Bitcoin mining. In other words, if more miners are vying for Bitcoin rewards, the protocol is coded to automatically increase mining difficulty.

Mining therefore requires powerful and competitive computing resources, which is why the hardware requirements are such a crucial component of the activity.



Download App for Android

Download App for iOS

Requirements To Become a Bitcoin Miner

For starters, you cannot use your everyday computer system to competitively mine Bitcoin. There are mining rigs that are purpose-built to deliver the level of computing power required to mine Bitcoin profitably, such as application specific integrated circuits (ASICs). Unfortunately, these mining rigs consume a lot of electricity. Hence, you also need to consider the overhead costs of powering and maintaining a mining rig. When you put all this together, you may discover that the capital required for successfully running a Bitcoin mining operation can quickly run into tens of thousands of dollars.

How Much Money Can a Bitcoin Miner Make?

After assessing the capital required to set up and maintain a Bitcoin mining rig, it's a good idea to evaluate your potential profitability. Note that you are currently entitled to receive 6.25 BTC whenever you succeed as the first miner to add a new block to the blockchain. This in addition to the fees that are paid to you with every 1 MB worth of transactions you verify.

Nonetheless, note that the probability of earning rewards as a solo miner is low, especially if you do not have the capital to set up a large mining farm. To boost their earning power, miners therefore often join Bitcoin mining pools. These pools are similar to a Powerball club, whose members agree to combine their funds to buy lotto tickets en masse with the agreement to share any proceeds in the case of a win.

In the case of a mining pool, the members combine their computing power in order to significantly increase their chances of earning newly minted Bitcoins. The revenue is shared among members in accordance with an agreed ratio.



The Risks of Bitcoin Mining

As well as evaluating your potential profitability, don't forget to consider all of the risks involved in Bitcoin mining. The most prevalent risk at the moment centers around regulation. We have begun to witness an increasing number of cities and states making moves to ban Bitcoin mining. A prominent example is New York, which is currently on the verge of passing a bill against Bitcoin mining activities.

It would be devastating to spend thousands of dollars on setting up a Bitcoin mining business only to have your government ban such activities. It's therefore advisable to thoroughly research your country's stance on cryptocurrency and related activities before investing in any Bitcoin mining equipment.

Please also note that joining a mining pool does not necessarily mean that you will automatically make a profit. As mentioned before, you must consider ongoing electricity expenses. You can use the online bitcoin mining calculator to roughly estimate your potential income.