# Bitcoin Mining

## What is Bitcoin?

Bitcoin is a consensus network that enables a new payment system and a completely digital money. It is the first decentralized peer-to-peer payment network that is powered by its users with no central authority or middlemen. From a user perspective, Bitcoin is pretty much like cash for the Internet.

## Are Bitcoin and Blockchain Similar?


- Blockchain is not Bitcoin, but it is the technology behind Bitcoin.
- Bitcoin is the digital token and blockchain is the ledger to keep track of who owns the digital tokens.
- One can't have Bitcoin without blockchain but can have blockchain without Bitcoin.

## What is Bitcoin Mining and How it Works?

Mining is the process of spending computing power to process transactions, secure the network, and keep everyone in the system synchronized together. It can be perceived like the Bitcoin data center except that it has been designed to be fully decentralized with miners operating in all countries and no individual having control over the network. This process is referred to as "mining" as an analogy to gold mining because it is also a temporary mechanism used to issue new bitcoins. Unlike gold mining, however, Bitcoin mining provides a reward in exchange for useful services required to operate a secure payment network. Mining will still be required after the last bitcoin is issued.

The bitcoin mining process serves two purposes in bitcoin:

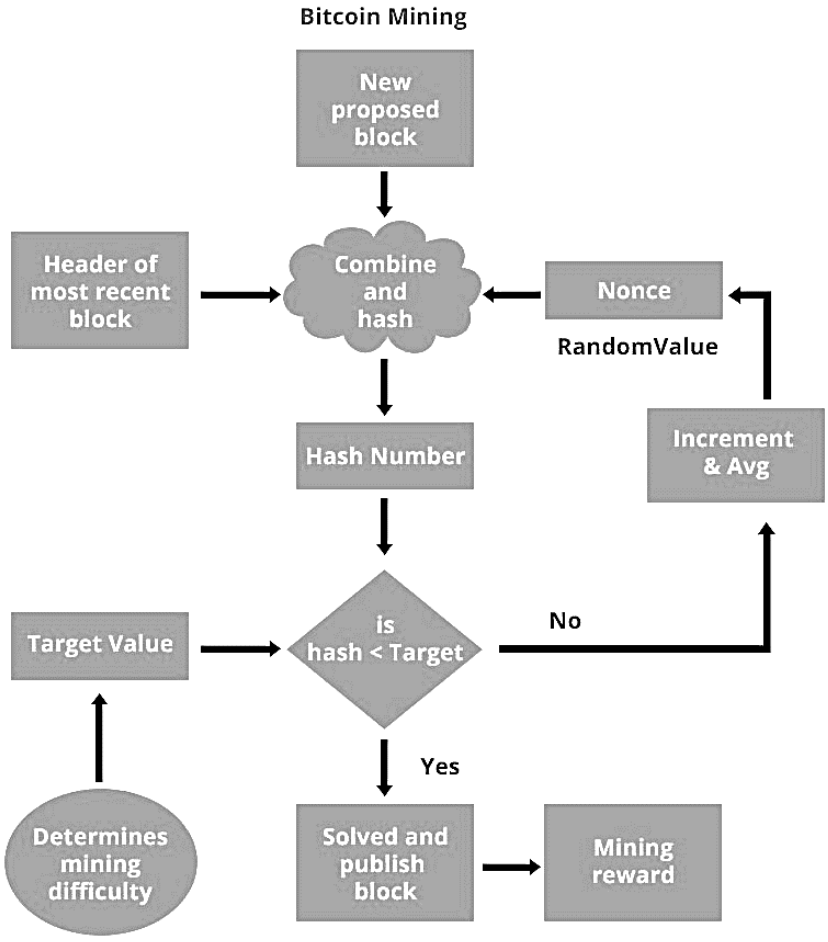
- Mining creates new bitcoins in each block, almost like a central bank printing new money. The amount of bitcoin created per block is fixed and diminishes with time.
- Mining creates trust by ensuring that transactions are only confirmed if enough computational power was devoted to the block that contains them. More blocks mean more computation, which means more trust.

Anybody can become a Bitcoin miner by running software with specialized hardware. Mining software listens for transactions broadcast through the peer-to-peer network and performs appropriate tasks to process and confirm these transactions. Bitcoin miners perform this work because they can earn transaction fees paid by users for faster transaction processing, and newly created bitcoins issued into existence according to a fixed formula.

For new transactions to be confirmed, they need to be included in a block along with a mathematical proof of work. Such proofs are very hard to generate because there is no way to create them other than by trying billions of calculations per second. This requires miners to perform these calculations before their blocks are accepted by the network and before they are rewarded.

The proof of work is also designed to depend on the previous block to force a chronological order in the blockchain. This makes it exponentially difficult to reverse previous transactions because this requires the recalculation of the proofs of work of all the subsequent blocks. When two blocks are found at the same time, miners work on the first block they receive and switch to the longest chain of blocks as soon as the next block is found. This allows mining to secure and maintain a global consensus based on processing power.

A simple block diagram is given below to illustrate how a new block is added in the networks through bitcoin mining and how a user getting the reward.



## How Bitcoin Miners Ensures Security in Bitcoin Network?

Bitcoin miners help keep the Bitcoin network secure by approving transactions. Mining is an important and integral part of Bitcoin that ensures fairness while keeping the Bitcoin network stable, safe and secure. Bitcoin nodes use the blockchain to distinguish legitimate Bitcoin transactions from attempts to re-spend coins that have already been spent elsewhere.

Bitcoin mining is intentionally designed to be resource-intensive and difficult so that the number of blocks found each day by miners remains steady. Individual blocks must contain a proof of work to be considered valid. This proof of work is verified by other Bitcoin nodes each time they receive a block. Bitcoin uses the hashcash proof-of-work function.

The bitcoin mining process serves two purposes in bitcoin:

- Mining creates new bitcoins in each block, almost like a central bank printing new money. The amount of bitcoin created per block is fixed and diminishes with time.
- Mining creates trust by ensuring that transactions are only confirmed if enough computational power was devoted to the block that contains them. More blocks mean more computation, which means more trust.

This both serves the purpose of disseminating new coins in a decentralized manner as well as motivating people to provide security for the system.

## What Do You Mean by Bitcoin Mining Difficulty?

### The Computationally-Difficult Problem

Bitcoin mining a block is difficult because the SHA-256 hash of a block's header must be lower than or equal to the target in order for the block to be accepted by the network.

This problem can be simplified for explanation purposes: The hash of a block must start with a certain number of zeros. The probability of calculating a hash that starts with many zeros is very low, therefore many attempts must be made. In order to generate a new hash each round, a nonce is incremented. See Proof of work for more information.

### The Bitcoin Network Difficulty Metric

The Bitcoin mining network difficulty is the measure of how difficult it is to find a new block compared to the easiest it can ever be. It is recalculated every 2016 blocks to a value such that the previous 2016 blocks would have been generated in exactly two weeks had everyone been mining at this difficulty. This will yield, on average, one block every ten minutes.

As more miners join, the rate of block creation will go up. As the rate of block generation goes up, the difficulty rises to compensate which will push the rate of block creation back down. Any blocks released by malicious miners that do not meet the required difficulty target will simply be rejected by everyone on the network and thus will be worthless.

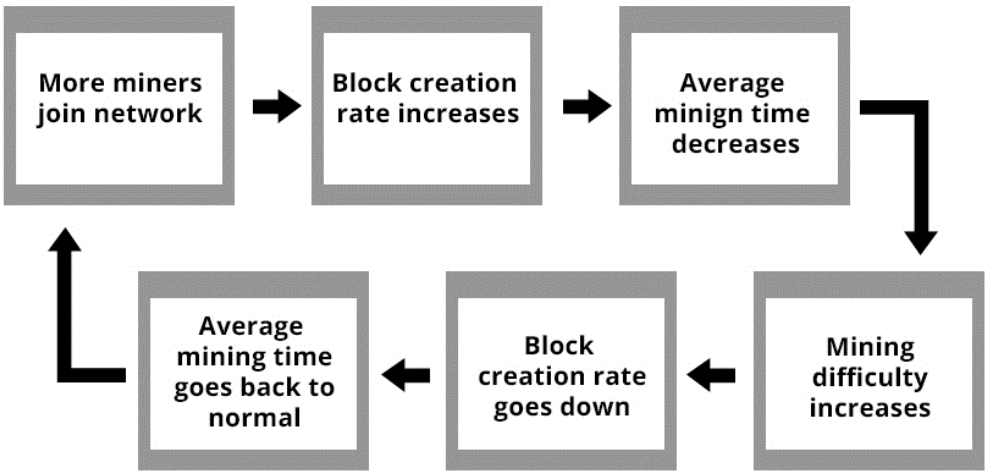
**The Block Reward**

When a block is discovered, the discoverer may award themselves a certain number of bitcoins, which is agreed-upon by everyone in the network. Currently, this bounty is 25 bitcoins; this value will halve every 210,000 blocks. See Controlled Currency Supply.

Additionally, the miner is awarded the fees paid by users sending transactions. The fee is an incentive for the miner to include the transaction in their block. In the future, as the number of new bitcoins miners are allowed to create in each block dwindles, the fees will make up a much more important percentage of mining income.

## How is Bitcoin Maintaining Average Mining Time?

As more miners join, the rate of block creation will go up. As the rate of block generation goes up, the difficulty rises to compensate which will push the rate of block creation back down. Any blocks released by malicious miners that do not meet the required difficulty target will simply be rejected by everyone on the network and thus will be worthless. As a result, mining is a very competitive business where no individual miner can control what is included in the blockchain.




## What Do You Mean by Hashing? Write Down the Properties Required for Cryptographic Hash Functions?

Hashing is one way to enable security during the process of message transmission when the message is intended for a particular recipient only. In simple terms, hashing means taking an input string of any length and giving out an output of a fixed length which helps to protect the security of the transmission against tampering. In the context of cryptocurrencies like Bitcoin, the transactions are taken as an input and run through a hashing algorithm (Bitcoin uses SHA-256) which gives an output of a fixed length.

## Properties Required for Cryptographic Hash Functions:

A cryptographic hash function is a special class of hash functions which has various properties making it ideal for cryptography. There are certain properties that a cryptographic hash function needs to have in order to be considered secure. Let's run through them one by one.

**Property 1: Deterministic**

This means that no matter how many times you parse through a particular input through a hash function you will always get the same result. This is critical because if you get different hashes every single time it will be impossible to keep track of the input.

**Property 2: Quick Computation**

The hash function should be capable of returning the hash of an input quickly. If the process isn't fast enough then the system simply won't be efficient.

**Property 3: Pre-Image Resistance**

What pre-image resistance states are that given H(A) it is infeasible to determine A, where A is the input and H(A) is the output hash. Notice the use of the word "infeasible" instead of "impossible". We already know that it is not impossible to determine the original input from its hash value. Let's take an example.

Suppose you are rolling a dice and the output is the hash of the number that comes up from the dice. How will you be able to determine what the original number was? It's simple all that you have to do is to find out the hashes of all numbers from 1-6 and compare. Since hash functions are deterministic, the hash of a particular input will always be the same, so you can simply compare the hashes and find out the original input.

But this only works when the given amount of data is very less. What happens when you have a huge amount of data? Suppose you are dealing with a 128-bit hash. The only method that you have to find the original input is by using the "brute-force method". Brute-force method basically means that you have to pick up a random input, hash it and then compare the output with the target hash and repeat until you find a match.

***So, what will happen if you use this method?***

***Best Case Scenario:***

You get your answer on the first try itself. You will seriously have to be the luckiest person in the world for this to happen. The odds of this happening are astronomical.

***Worst Case Scenario:***

You get your answer after 2^128 – 1 times. Basically, it means that you will find your answer at the end of all the data.

***Average Scenario:***

You will find it somewhere in the middle so basically after 2^128/2 = 2^127 times. To put that into perspective, 2^127 = 1.7 X 10^38. In other words, it is a huge number.

**Property 4: Small Changes In The Input Changes the Hash.**
Even if you make a small change in your input, the changes that will be reflected in the hash will be huge.

**Property 5: Collision Resistant**
Given two different inputs A and B where H(A) and H(B) are their respective hashes, it is infeasible for H(A) to be equal to H(B). What that means is that for the most part, each input will have its own unique hash. Why did we say "for the most part"? Let's talk about an interesting concept called "The Birthday Paradox".

Suppose you have a 128-bit hash which has 2^128 different possibilities. By using the birthday paradox, you have a 50% chance to break the collision resistance at the sqrt(2^128) = 2^64th instance.

As you can see, it is much easier to break collision resistance than it is to break pre-image resistance. No hash function is collision-free, but it usually takes so long to find a collision. So, if you are using a function like SHA-256, it is safe to assume that if H(A) = H(B) then A = B.

**Property 6: Puzzle Friendly**
Now, this is a fascinating property, and the application and impact that this one property has had on cryptocurrency are huge. For every output "Y", if k is chosen from a distribution with high min-entropy, it is infeasible to find an input x such that H(k|x) = Y.

That probably went all over your head! But it's ok, let's now understand what that definition means.

SHA 256: Produces a 256-bit hash. This is currently being used by Bitcoin.
Keccak-256: Produces a 256-bit hash and is currently used by Ethereum.

When the Bitcoin mining software wants to add a new block to the blockchain, this is the procedure it follows. Whenever a new block arrives, all the contents of the blocks are first hashed. If the hash is lesser than the difficulty target, then it is added to the blockchain and everyone in the community acknowledges the new block.

However, it is not as simple as that. You will have to be extremely lucky to get a new block just like that. This is where the nonce comes in. The nonce is an arbitrary string which is concatenated with the hash of the block. After that this concatenated string is hashed again and compared to the difficulty level. If it is not less than the difficulty level, then the nonce is changed and this keeps on repeating a million times until finally, the requirements are met. When that happens the block is added to the blockchain.

## Rest of the parts are optional (Probably for Leisure Reading) .....

## How to Obtain Bitcoin?

Understanding how Bitcoin works may be interesting to some, but you're probably wanting to know how you can acquire some bitcoins of your own. There are actually a few ways you can legally get bitcoins - no matter where you live in the world. As long as you have an Internet connection and the Bitcoin software installed, you're going to be able to begin using this virtual currency. The best news is that it's actually fairly easy to begin to build up your Bitcoin Wallet if you have a little spare time.

First, it should be noted that it's really difficult to purchase bitcoins with a credit card or PayPal account. This may seem odd at first, but if you think about it this makes sense. It's really easy to issue a chargeback on a credit card. If someone buys BTC with a credit card and then reverses the charge, it's really tough to prove to the credit card companies that the exchange really happened. Because of this, most major Bitcoin Exchanges do not allow you to purchase BTC with a credit card or PayPal account.

Okay, with that aside, let's dive in and look at the exact steps you're going to need to take in order to start amassing BTC of your own. It's important to remember that the value of one BTC is very volatile right now, so you probably don't want to invest everything you have in this virtual currency. At the same time, the popularity of Bitcoin is growing throughout the world and some people are already getting rich by building up large piles of bitcoins virtually via means and method we'll describe below.

**Step One: Get a Bitcoin Wallet**

The very first thing you're going to need is a Bitcoin Wallet - aka a Bitcoin client. No matter what type of computer you're running, there's going to be an installer program to get you up and running in no time at all. Most people find it takes around 5 to 10 minutes to get a Bitcoin client installed and connected to the network.

Be sure you take your time to find a client you're comfortable with using. Most are very similar, but some have some extra bells and whistles that might make it easier for you to get started. The most popular option for Windows, Mac, and Linux is currently MultiBit. Bitcoin Wallet for Android OS is also available.

Another option is to use a web-based Bitcoin Wallet, although this isn't really recommended. While you may be able to find a service that offers a high level of security, it's not the same level you'd have if you install the software on your own computer where you have complete control. Coinbase is one of the more popular online Bitcoin wallets currently.

Whichever you choose, once it's installed the next step is easy. You'll generate a public and private key. This is your Bitcoin address that will allow people to send BTC to your account. After you have your Bitcoin Wallet setup, you have a few different options on how to accrue BTC in your wallet. We're going to go over these - one by one - next.

**Bitcoin Exchanges**

Bitcoin exchanges weren't around when Bitcoin first came out, but they're now an integral part of how the whole Bitcoin ecosystem works. There are exchanges that include Bitcoin among other virtual currencies online as well as marketplaces that deal exclusively with BTC transactions.

It's interesting to note that some of these marketplaces will hold a balance for you - outside of your Bitcoin Wallet - in order to make it easier to conduct trades. Choosing the right Bitcoin Exchange is important if you want to stay safe and not risk losing your BTC balance due to a scam or technical problems.

Here's a look at the major factors you need to look at before choosing a Bitcoin Exchange.

- Security – The most important aspect you want to think about is security. If a Bitcoin Exchange is new to the Internet and is missing contact information, this is a good sign that they probably don't care too much about the security of your personal information. It's important to do your homework so that you can determine which Bitcoin Exchange website has the best track record when it comes to security. Luckily, if you spend any amount of time on the many Bitcoin forums and communities online, you'll see which exchanges have problems and which exchanges are recommended.
- Geography - While Bitcoin is a decentralized network that spreads around the globe, you still need to think about your physical location. For example, some Bitcoin Exchanges will not allow you to withdraw funds to a US bank account. It's a good idea to make sure whatever exchange you're thinking about using has a way for you to convert your BTC to your local currency easily and safely. In 2013, some people began complaining about the amount of time it took MtGox to transfer funds to the US, so it's a good idea to once again hit the forums and try to gauge public opinion about any exchange you're thinking of using.

Next, let's take a quick look at some of the major Bitcoin Exchanges currently operating. New ones are appearing all the time, but it's generally a safer bet working with one that has been around for a while and has managed to build up a track record of being reputable and honest.

- CoinBase – This is one of the most popular Bitcoin Exchanges at the moment. They offer the ability to transfer funds to US bank accounts. Having said that, if you live elsewhere in the world, you may not be happy about not being able to transfer funds to your local bank account.
- MtGox – At one time, MtGox was responsible for the majority of Bitcoin transactions in the world. This has changed recently as they've run into some legal problems in different countries around the world, but they're still a very popular Bitcoin Exchange that many people use on a daily basis.
- BTC-E – This website is based in an unknown city in Bulgaria, so you might be cautious about keeping any BTC here. The prices per BTC are generally a lot lower here, but this is because it takes a ridiculous amount of time to confirm a transaction. Still, it's an option you might look at depending on where you live currently.

- Bitstamp – This exchange is similar to CoinBase in a lot of ways. The main difference is that they do routinely work with people in countries other than the United States, making it easy to transfer BTC to foreign currencies. If you're looking for a truly global Bitcoin Exchange, this is a good place to start.
- Cryptsy – This isn't a pure Bitcoin Exchange. By that, we mean that you can trade other cryptocurrencies as well. For example, you can exchange your BTC for LTC (LiteCoins) and vice versa. If your virtual currency investments go beyond Bitcoin, you'll want to check out Cryptsy.
- BTer – With slow transaction speeds and limits on the size of transactions, this isn't really recommended, but we thought they deserved a spot on the list because they do serve the needs of some people who use Bitcoin.
- BTC-China – One of the fastest-growing Bitcoin exchanges – according to Wired magazine is BTC-China, which has really ramped up their efforts recently. By some accounts, they've overtaken MtGox as the place where most Bitcoin transactions take place on a daily basis.

## Face to Face / Over the Counter Trades:

Even though it's a virtual currency, you can still arrange to meet someone in person and conduct a transaction with them. Having said that, finding such people might be difficult. This is where the LocalBitcoins.com website comes into the picture. LocalBitcoins is the main website people use to find people who want to meet face to face to exchange bitcoins for cash or vice versa. The website even allows them to negotiate prices beforehand. Add in an escrow service, and it's one of the easiest and safest places to find someone to exchange bitcoins with locally.

No matter the value of the money being exchanged, it's important for you to stay safe. To do this, it's a good idea to always arrange to meet in a public place surrounded by a lot of people. Never agree to go to someone's home, apartment, or a field on the outside of town! In all seriousness, use your common sense when setting up a face to face Bitcoin transaction. Even though you're meeting in the real world, you're still going to need access to your Bitcoin Wallet. Once you have the cash, use the other person's Bitcoin Address to send them the predetermined amount of bitcoins. The good news is that you can use a laptop, tablet or even your smartphone to do this wherever you are as long as you have a WiFi connection.

In addition to one on one meetings, many people around the world also have Bitcoin groups that meet in public places in order to exchange Bitcoin for cash and vice versa. Websites like Meetup.com routinely have Bitcoin groups that meet in real life. In some big cities, you may find multiple groups meeting on different days of the month. Additionally, you may find so-called "Satoshi Squares" or Bitcoin markets set-up in public places.

It should be noted that in most cases you're going to pay a transaction fee of 5% to 10% (or more) to the seller in exchange for the privacy and immediacy. This is too much for some people, but for others, it's just a cost of doing business. Just be sure the local police don't think you're exchanging money for illicit substances!