



[CRYPTOCURRENCY](#) > [BITCOIN](#)

How Does Bitcoin Mining Work?



By [ADAM HAYES](#) | Updated Nov 21, 2019

☰ TABLE OF CONTENTS

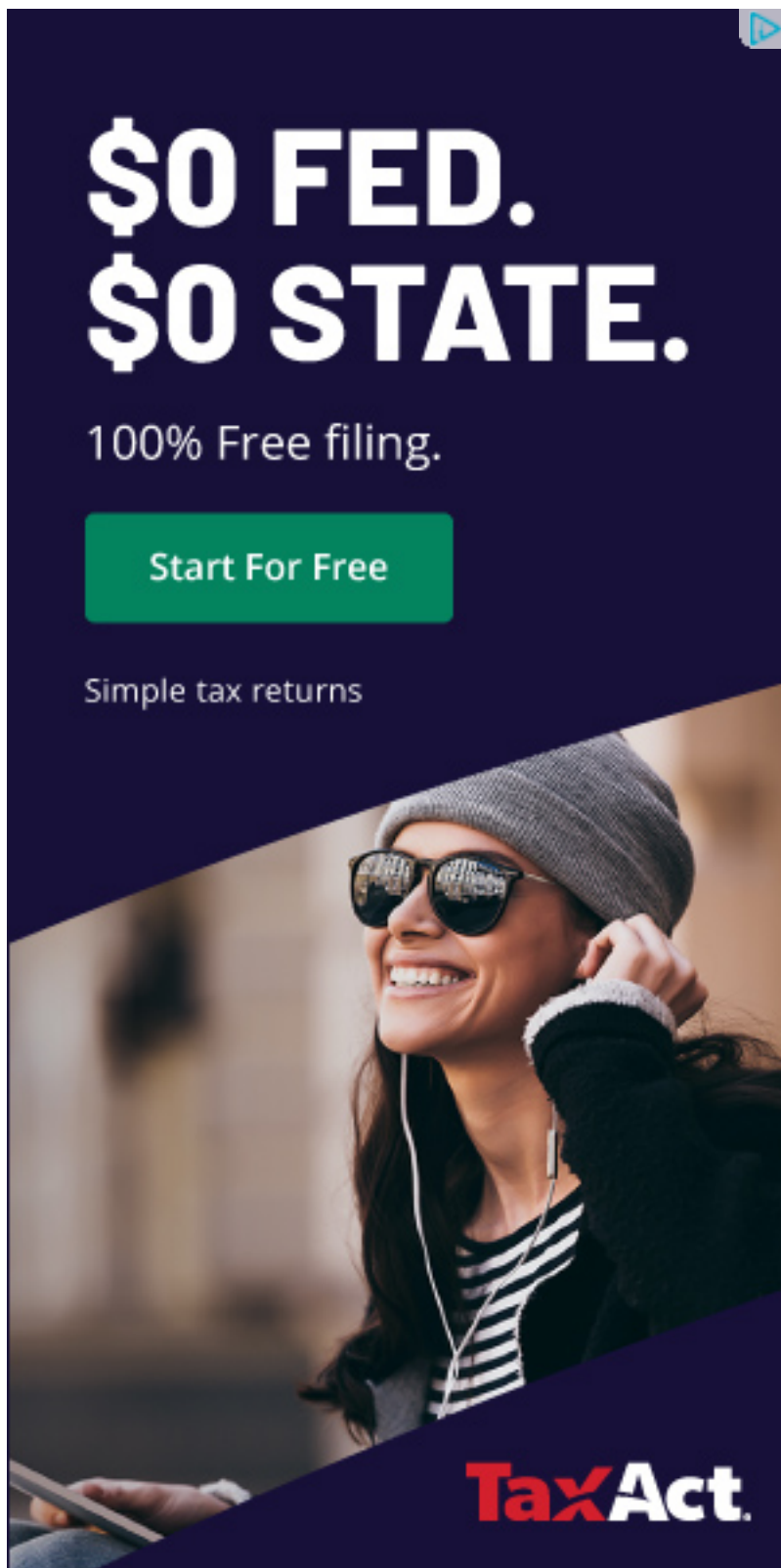
- ↪ [What is Bitcoin Mining?](#)
- ↪ [What Coin Miners Actually Do](#)
- ↪ [Mining and Bitcoin Circulation](#)

EXPAND +

What is Bitcoin Mining?

[Cryptocurrency](#) mining is painstaking, costly and only sporadically rewarding. Nonetheless, mining has a magnetic appeal for many investors interested in cryptocurrency because of the fact that miners are rewarded for their work with crypto tokens. This may be because entrepreneurial types see mining as pennies from heaven, like California gold prospectors in 1849. And if you are technologically inclined, why not do it?

However, before you invest the time and equipment, read this explainer to see whether mining is really for you. We will focus primarily on Bitcoin (throughout, we'll use "Bitcoin" when referring to the network or the cryptocurrency as a concept, and "bitcoin" when we're referring to a quantity of individual tokens).



**\$0 FED.
\$0 STATE.**

100% Free filing.

Start For Free

Simple tax returns

TaxAct.

The primary draw for many Bitcoin miners is the prospect of being rewarded with valuable bitcoin tokens. That said, you certainly don't have to be a miner to own cryptocurrency tokens. You can also [buy](#)

[cryptocurrencies using fiat currency](#); you can trade it on an exchange like [Bitstamp](#) using another crypto (as an example, using Ethereum or NEO to buy bitcoin); you even can earn it by playing video games or by publishing blog posts on platforms that pay users in cryptocurrency. An example of the latter is [Steemit](#), which is kind of like Medium except that users can reward bloggers by paying them in a proprietary cryptocurrency called STEEM. STEEM can then be traded elsewhere for bitcoin.

Advertisement

Advertisement

The bitcoin reward that miners receive is an incentive which motivates people to assist in the primary purpose of mining: to support, legitimize and monitor the Bitcoin network and its blockchain. Because these responsibilities are spread among many users all over the world, bitcoin is said to be a "decentralized" cryptocurrency, or one that does not rely on a central bank or government to oversee its regulation.

KEY TAKEAWAYS

- By mining, you can earn cryptocurrency without having to put down money for it.
- Bitcoin miners receive bitcoin as a reward for completing "blocks" of verified transactions which are added to the blockchain.
- Mining rewards are paid to the miner who discovers a solution to a

complex hashing puzzle first, and the probability that a participant will be the one to discover the solution is related to the portion of the total mining power on the network.

- Double spending is a phenomenon in which a bitcoin user illicitly spends the same tokens twice.
- You need either a GPU (graphics processing unit) or an application-specific integrated circuit (ASIC) in order to set up a mining rig.

What Coin Miners Actually Do

Miners are getting paid for their work as auditors. They are doing the work of verifying previous bitcoin transactions. This convention is meant to keep Bitcoin users honest and was conceived by bitcoin's founder, [Satoshi Nakamoto](#). By verifying transactions, miners are helping to prevent the "[double-spending](#) problem."

Double spending is a scenario in which a bitcoin owner illicitly spends the same bitcoin twice. With physical currency, this isn't an issue: once you hand someone a \$20 bill to buy a bottle of vodka, you no longer have it, so

there's no danger you could use that same \$20 bill to buy lotto tickets next door. With digital currency, however, as the Investopedia dictionary explains, "there is a risk that the holder could make a copy of the digital token and send it to a merchant or another party while retaining the original."

Let's say you had one legitimate \$20 bill and one counterfeit of that same \$20. If you were to try to spend both the real bill and the fake one, someone that took the trouble of looking at both of the bills' serial numbers would see that they were the same number, and thus one of them had to be false. What a bitcoin miner does is analogous to that—they check transactions to make sure that users have not illegitimately tried to spend the same bitcoin twice. This isn't a perfect analogy—we'll explain in more detail below.

Once a miner has verified 1 MB (megabyte) worth of [bitcoin transactions](#), known as a "block," that miner is eligible to be rewarded with a quantity of bitcoin (more about the bitcoin reward below as well). The 1 MB limit was set by Satoshi Nakamoto, and is a matter of controversy, as some miners believe the block size should be increased to accommodate more data,

which would effectively mean that the bitcoin network could process and verify transactions more quickly.

Note that verifying 1 MB worth of transactions makes a coin miner eligible to earn bitcoin—not everyone who verifies transactions will get paid out.

1MB of transactions can theoretically be as small as one transaction (though this is not at all common) or several thousand. It depends on how much data the transactions take up.

"So after all that work of verifying transactions, I might still not get any bitcoin for it?"

That is correct.

To earn bitcoins, you need to meet two conditions. One is a matter of effort; one is a matter of luck.

- 1) You have to verify ~1MB worth of transactions. This is the easy part.
- 2) You have to be the *first* miner to arrive at the right answer to a numeric problem. This process is also known as [proof of work](#).

"What do you mean, 'the right answer to a numeric problem'?"

The good news: No advanced math or computation is involved. You may have heard that miners are solving difficult mathematical problems—that's not exactly true. What they're actually doing is trying to be the first miner to come up with a 64-digit hexadecimal number (a "[hash](#)") that is less than or equal to the target hash. It's basically guesswork.

The bad news: It's guesswork, but with the total number of possible guesses for each of these problems being on the order of trillions, it's incredibly arduous work. In order to solve a problem first, miners need a lot of computing power. To mine successfully, you need to have a high "hash rate," which is measured in terms of megahashes per second (MH/s), gigahashes per second (GH/s), and terahashes per second (TH/s).

That is a great many hashes.

If you want to estimate how much bitcoin you could mine with your mining

rig's hash rate, the site [Cryptocompare](#) offers a helpful calculator.

Mining and Bitcoin Circulation

In addition to lining the pockets of miners and supporting the bitcoin ecosystem, mining serves another vital purpose: It is the only way to release new cryptocurrency into circulation. In other words, miners are basically "minting" currency. For example, as of Nov. 2019, there were around 18 million bitcoins in circulation. ^[1] Aside from the coins minted via the genesis block (the very first block, which was created by founder Satoshi Nakamoto), every single one of those bitcoin came into being because of miners. In the absence of miners, Bitcoin as a network would still exist and be usable, but there would never be any additional bitcoin. There will eventually come a time when bitcoin mining ends; per the Bitcoin Protocol, the total number of bitcoins will be capped at 21 million. ^[2] However, because the rate of bitcoin "mined" is reduced over time, the final bitcoin won't be circulated until around the year 2140.


Aside from the short-term bitcoin payoff, being a coin miner can give you "voting" power when changes are proposed in the Bitcoin network protocol. In other words, a successful miner has an influence on the decision-making process on such matters as [forking](#).

How Much a Miner Earns

The rewards for bitcoin mining are halved every four years or so. When bitcoin was first mined in 2009, mining one block would earn you 50 BTC. In 2012, this was halved to 25 BTC. By 2016, this was halved again to the current level of 12.5 BTC. In about 2020, the reward size will be halved again to 6.25 BTC. As of the time of writing, the reward for completing a block is

12.5 Bitcoin. In November of 2019, the price of Bitcoin was about \$9,300 per bitcoin, which means you'd earn \$116,250 ($12.5 \times 9,300$) for completing a block.^[3] Not a bad incentive to solve that complex hash problem detailed above, it might seem.

Bitcoin Mining Rewards



If you want to keep track of precisely when these halvings will occur, you can consult the [Bitcoin Clock](#), which updates this information in real time. Interestingly, the market price of bitcoin has, throughout its history, tended to correspond closely to the marginal cost of mining a bitcoin.

If you are interested in seeing how many blocks have been mined thus far, there are several sites, including [Blockchain.info](https://blockchain.info), that will give you that information in real time.

Equipment Needed to Mine

Although early on in bitcoin's history individuals may have been able to compete for blocks with a regular at-home computer, this is no longer the case. The reason for this is that the difficulty of mining bitcoin changes over time. In order to ensure smooth functioning of the blockchain and its ability to process and verify transaction, the Bitcoin network aims to have one block produced every 10 minutes or so. However, if there are one million mining rigs competing to solve the hash problem, they'll likely reach a solution faster than a scenario in which 10 mining rigs are working on the same problem. For that reason, Bitcoin is designed to evaluate and adjust the difficulty of mining every 2,016 blocks, or roughly every two weeks. When there is more computing power collectively working to mine for bitcoin, the difficulty level of mining increases in order to keep block production at a stable rate. Less computing power means the difficulty level decreases. To get a sense of just how much computing power is involved, when Bitcoin launched in 2009 the initial difficulty level was one. As of Nov. 2019, it is more than 13 trillion.

All of this is to say that, in order to mine competitively, miners must now invest in powerful computer equipment like a GPU (graphics processing unit) or, more realistically, an application-specific integrated circuit (ASIC). These can run from \$500 to the tens of thousands. Some miners—particularly Ethereum miners—buy individual graphics cards (GPUs) as a low-cost way to cobble together mining operations. The photo below is a

makeshift, home-made mining machine. The graphics cards are those rectangular blocks with whirring circles. Note the sandwich twist-ties holding the graphics cards to the metal pole. This is probably not the most efficient way to mine, and as you can guess, many miners are in it as much for the fun and challenge as for the money.

Bitcoin



Shutterstock

The "Explain It Like I'm Five" Version

The ins and outs of bitcoin mining can be difficult to understand as is. Consider this illustrative example for how the hash problem works: I tell three friends that I'm thinking of a number between one and 100, and I write that number on a piece of paper and seal it in an envelope. My friends don't have to guess the exact number; they just have to be the first person

to guess any number that is less than or equal to the number I am thinking of. And there is no limit to how many guesses they get.

Let's say I'm thinking of the number 19. If Friend A guesses 21, they lose because of $21 > 19$. If Friend B guesses 16 and Friend C guesses 12, then they've both theoretically arrived at viable answers, because of $16 < 19$ and $12 < 19$. There is no "extra credit" for Friend B, even though B's answer was closer to the target answer of 19. Now imagine that I pose the "guess what number I'm thinking of" question, but I'm not asking just three friends, and I'm not thinking of a number between 1 and 100. Rather, I'm asking millions of would-be miners and I'm thinking of a 64-digit hexadecimal number. Now you see that it's going to be extremely hard to guess the right answer.

If B and C both answer simultaneously, then the ELI5 analogy breaks down.

In Bitcoin terms, simultaneous answers occur frequently, but at the end of the day, there can only be one winning answer. When multiple simultaneous answers are presented that are equal to or less than the target number, the Bitcoin network will decide by a simple majority—51%—which miner to honor. Typically, it is the miner who has done the most work, that is, the one that verifies the most transactions. The losing block then becomes an "[orphan block](#)." Orphan blocks are those that are not added to the blockchain. Miners who successfully solve the hash problem but who haven't verified the most transactions are not rewarded with bitcoin.

What Is a "64-Digit Hexadecimal Number"?

Well, here is an example of such a number:

The number above has 64 digits. Easy enough to understand so far. As you probably noticed, that number consists not just of numbers, but also letters of the alphabet. Why is that?

To understand what these letters are doing in the middle of numbers, let's unpack the word "hexadecimal."

As you know, we use the "decimal" system, which means it is base 10. This, in turn, means that every digit of a multi-digit number has 10 possibilities, zero through nine.

"Hexadecimal," on the other hand, means base 16, as "hex" is derived from the Greek word for six and "deca" is derived from the Greek word for 10. In a hexadecimal system, each digit has 16 possibilities. But our numeric system only offers 10 ways of representing numbers (zero through nine). That's why you have to stick letters in, specifically letters a, b, c, d, e and f.

If you are mining bitcoin, you do not need to calculate the total value of that 64-digit number (the hash). I repeat: You do not need to calculate the total value of a hash.

So, what do "64-digit hexadecimal numbers" have to do with bitcoin mining?

Remember that ELI5 analogy, where I wrote the number 19 on a piece of paper and put it in a sealed envelope?

In bitcoin mining terms, that metaphorical undisclosed number in the envelope is called the [target hash](#).

What miners are doing with those huge computers and dozens of cooling fans is guessing at the target hash. Miners make these guesses by randomly generating as many "[nonces](#)" as possible, as fast as possible. A nonce is short for "number only used once," and the nonce is the key to generating these 64-bit hexadecimal numbers I keep talking about. In Bitcoin mining, a nonce is 32 bits in size—much smaller than the hash, which is 256 bits. The first miner whose nonce generates a hash that is less than or equal to the target hash is awarded credit for completing that block and is awarded the spoils of 12.5 BTC.

In theory, you could achieve the same goal by rolling a 16-sided die 64 times to arrive at random numbers, but why on earth would you want to do that?

The screenshot below, taken from the site [Blockchain.info](#), might help you put all this information together at a glance. You are looking at a summary of everything that happened when block #490163 was mined. The nonce that generated the "winning" hash was 731511405. The target hash is shown on top. The term "Relayed by Antpool" refers to the fact that this particular block was completed by AntPool, one of the more successful mining pools (more about mining pools below). As you see here, their contribution to the [Bitcoin community](#) is that they confirmed 1768 transactions for this block. If you really want to see all 1768 of those transactions for this block, go to [this page](#) and scroll down to the heading "Transactions."

(source: Blockchain.info)

"So how do I guess at the target hash?"

All target hashes begin with zeros—at least eight zeros and up to 63 zeros.

There is no minimum target, but there is a maximum target set by the Bitcoin Protocol. No target can be greater than this number:

00000000ffff000

Here are some examples of randomized hashes and the criteria for whether they will lead to success for the miner:



(Note: These are made-up hashes)

"How do I maximize my chances of guessing the target hash before anyone else does?"

You'd have to get a fast mining rig, or, more realistically, join a mining pool—a group of coin miners who combine their computing power and split the mined [bitcoin](#). Mining pools are comparable to those Powerball clubs whose members buy lottery tickets en masse and agree to share any winnings. A disproportionately large number of blocks are mined by pools rather than by individual miners.

In other words, it's literally just a numbers game. You cannot guess the pattern or make a prediction based on previous target hashes. The [difficulty level](#) of the most recent block at the time of writing is about 13.69 trillion, meaning that the chance of any given nonce producing a hash below the target is one in 13.69 trillion. Not great odds if you're working on your own, even with a tremendously powerful mining rig.

"How do I decide whether bitcoin will be profitable for me?"

Not only do miners have to factor in the costs associated with expensive equipment necessary to stand a chance of solving a hash problem. They must also consider the significant amount of electrical power mining rigs utilize in generating vast quantities of nonces in search of the solution. All told, bitcoin mining is largely unprofitable for most individual miners as of this writing. The site [Cryptocompare](#) offers a helpful calculator that allows you to plug in numbers such as your hash speed and electricity costs to

estimate the costs and benefits.



(Source: Cryptocompare)

What Are Coin Mining Pools?

Mining rewards are paid to the miner who discovers a solution to the puzzle first, and the probability that a participant will be the one to discover the solution is equal to the portion of the total mining power on the network. Participants with a small percentage of the mining power stand a very small chance of discovering the next block on their own. For instance,

a mining card that one could purchase for a couple of thousand dollars would represent less than 0.001% of the network's mining power. With such a small chance at finding the next block, it could be a long time before that miner finds a block, and the difficulty going up makes things even worse. The miner may never recoup their investment. The answer to this problem is mining pools. Mining pools are operated by [third parties](#) and coordinate groups of miners. By working together in a pool and sharing the payouts among all participants, miners can get a steady flow of bitcoin starting the day they activate their miner. Statistics on some of the mining pools can be seen on [Blockchain.info](#).

"I've done the math. Forget mining. Is there a less onerous way to profit from cryptocurrencies?"

As mentioned above, the easiest way to acquire bitcoin is to buy it on an exchange like Coinbase.com. Alternately, you can always leverage the "pickaxe strategy." This is based on the old saw that during the 1849 California gold rush, the smart investment was not to pan for gold, but rather to make the pickaxes used for mining. Or, to put it in modern terms,

the pickaxes used for mining. Or, to put it in modern terms, the those pickaxes. In a equivalent would be a company that in mining. You may consider equipment or GPUs instead, for



Save More for Retirement When You Hire a Pro SPONSORED

The right financial advisor can help you [reach your long-term financial goals](#). SmartAsset's free tool matches you with [fiduciary financial advisors](#)



THE 2019

NISSAN TITAN XD®

Compare Financial

[started now.](#)

Hire Pro: Compare Financial Advisors In Your Area

financial advisor that [fits your needs](#) doesn't have to be hard. SmartAsset's free tool matches you with [fiduciary financial advisors](#) in your area in 5 minutes. Each advisor has been vetted by SmartAsset and is legally bound to act in your best interests. If you're ready to be matched with local advisors that will help you achieve your financial goals, [get started now.](#)

Advertisement

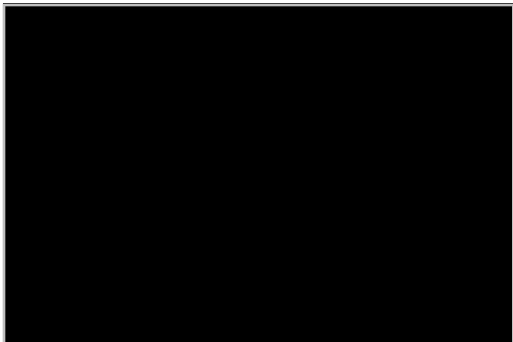
ARTICLE SOURCES ▼

Compare Accounts

[Advertiser Disclosure](#)

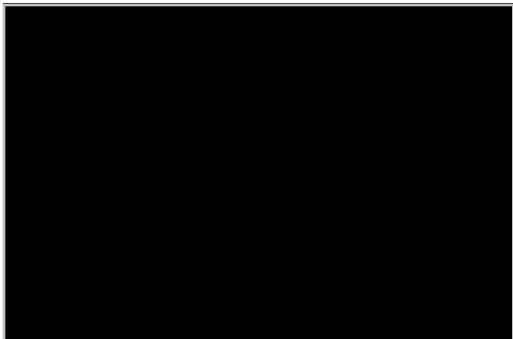


Related Articles



BITCOIN

How Bitcoin Works



BLOCKCHAIN

How does a block chain prevent double-spending of Bitcoins?

CRYPTOCURRENCY STRATEGY & EDUCATION
How to Choose a Cryptocurrency Mining Pool



BITCOIN
Is Bitcoin Mining Still Profitable?



BITCOIN
What Happens to Bitcoin After All 21 Million Are Mined?



BITCOIN
What Determines the Price of 1 Bitcoin?



\$1.50
per futures
contract

charles
SCHWAB

TD Ameritrade

TD Ameritrade

\$0.00

IG

MULTIPLE COINS

Seamlessly connect w/ the markets & your accounts on the award-winning E*TRADE Mobile app
Buy, Sell, & Trade Cryptocurrencies Across Multiple Markets Simultaneously.

Get access to TD Ameritrade's free education with videos, articles, and more.

Get a free personalized learning experience with TD Ameritrade.

Buy, Sell, & Trade Cryptocurrencies Across Multiple Markets Simultaneously.

Seamlessly connect w/ the markets on the E*TRADE Mobile app

Related Terms

Bitcoin Mining, Explained

Breaking down everything you need to know about Bitcoin mining, from blockchain and block rewards to Proof-of-Work and mining pools. [more](#)

Nonce Definition

Nonce is a number added to a hashed block, that, when rehashed, meets the difficulty level restrictions. [more](#)

Understanding Block Time in Cryptocurrency

Block time in the context of cryptocurrency is the average amount of time it takes for a new block to be added to a blockchain. [more](#)

Mining Pool Definition

A mining pool is a joint group of cryptocurrency miners who combine their computational resources over a network. [more](#)

Understanding Hash

A hash is a function that converts an input of letters and numbers into an encrypted output of a fixed length. [more](#)

ASIC Bitcoin Miner Definition

An application-specific integrated circuit (ASIC) bitcoin miner is a computerized device that was designed for the sole purpose of mining bitcoins. [more](#)



[About Us](#)

[Editorial Policy](#)

[Privacy Policy](#)

[California Privacy Notice](#)

[Terms of Use](#)

[Advertise](#)

[Contact Us](#)

[Dictionary](#)

[News](#)

[Careers](#)



Investopedia is part of the [Dotdash](#) publishing family.