SAINTS PERSPECTIVES
Things Scientific and Technical

How Does Bitcoin Mining Work?

https://www.investopedia.com/tech/how-does-bitcoin-mining-work/

An Investopedia Article
By EUNY HONG and Reviewed by JULIUS MANSA

September 21, 2021

What Is Bitcoin Mining?

Bitcoin mining is the process by which new **bitcoins** are entered into circulation; it is also the way that new transactions are confirmed by the network and a critical component of the maintenance and development of the blockchan ledger. "Mining" is performed using sophisticated hardware that solves an extremely complex computational math problem. The first computer to find the solution to the problem is awarded the next **block** of bitcoins and the process begins again.

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).

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.
- You need either a GPU (graphics processing unit) or an application-specific integrated circuit (ASIC) in order to set up a mining rig.

SAINTS PERSPECTIVES
Things Scientific and Technical

A New Gold Rush

The primary draw for many mining is the prospect of being rewarded with Bitcoin. 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 shopping, publishing blog posts on platforms that pay users in cryptocurrency, or even set up interest-earning crypto accounts.

An example of a crypto blog platform is **Steemi**t, 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.

The Bitcoin reward that miners receive is an incentive that motivates people to assist in the primary purpose of mining: to legitimize and monitor Bitcoin transactions, ensuring their validity. Because these responsibilities are spread among many users all over the world, Bitcoin is a "decentralized" cryptocurrency, or one that does not rely on any central authority like a central bank or government to oversee its regulation.

Mining to Prevent Double Spend

Miners are getting paid for their work as auditors. They are doing the work of verifying the legitimacy of Bitcoin transactions. This convention is meant to keep Bitcoin users honest and was conceived by Bitcoin's founder, Satoshi Nakamoto.1 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. While there is the possibility of counterfeit cash being made, it is not exactly the same as literally spending the same dollar twice. 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.

NOTE:
Only 1 megabyte of transaction data can fit into a single bitcoin block. The 1 MB limit was set by **Satoshi Nakamoto**, and this has become 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.

"So after all that work spent mining, I might still not get any bitcoin for it?"

That is correct. To earn bitcoins, you need to be the first miner to arrive at the right answer, or closest answer, to a numeric problem. This process is also known as proof of work (PoW).

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

The good news: No advanced math or computation is really involved. You may have heard that miners are solving difficult mathematical problems—that's true but not because the math itself is hard. 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 a matter of guesswork or randomness, but with the total number of possible guesses for each of these problems being on the order of trillions, it's incredibly arduous work. And the number of possible solutions only increases the more miners that join the mining network (known as the mining difficulty). 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 gigahashes per second (GH/s) and terahashes per second (TH/s).

Mining and Bitcoin Circulation

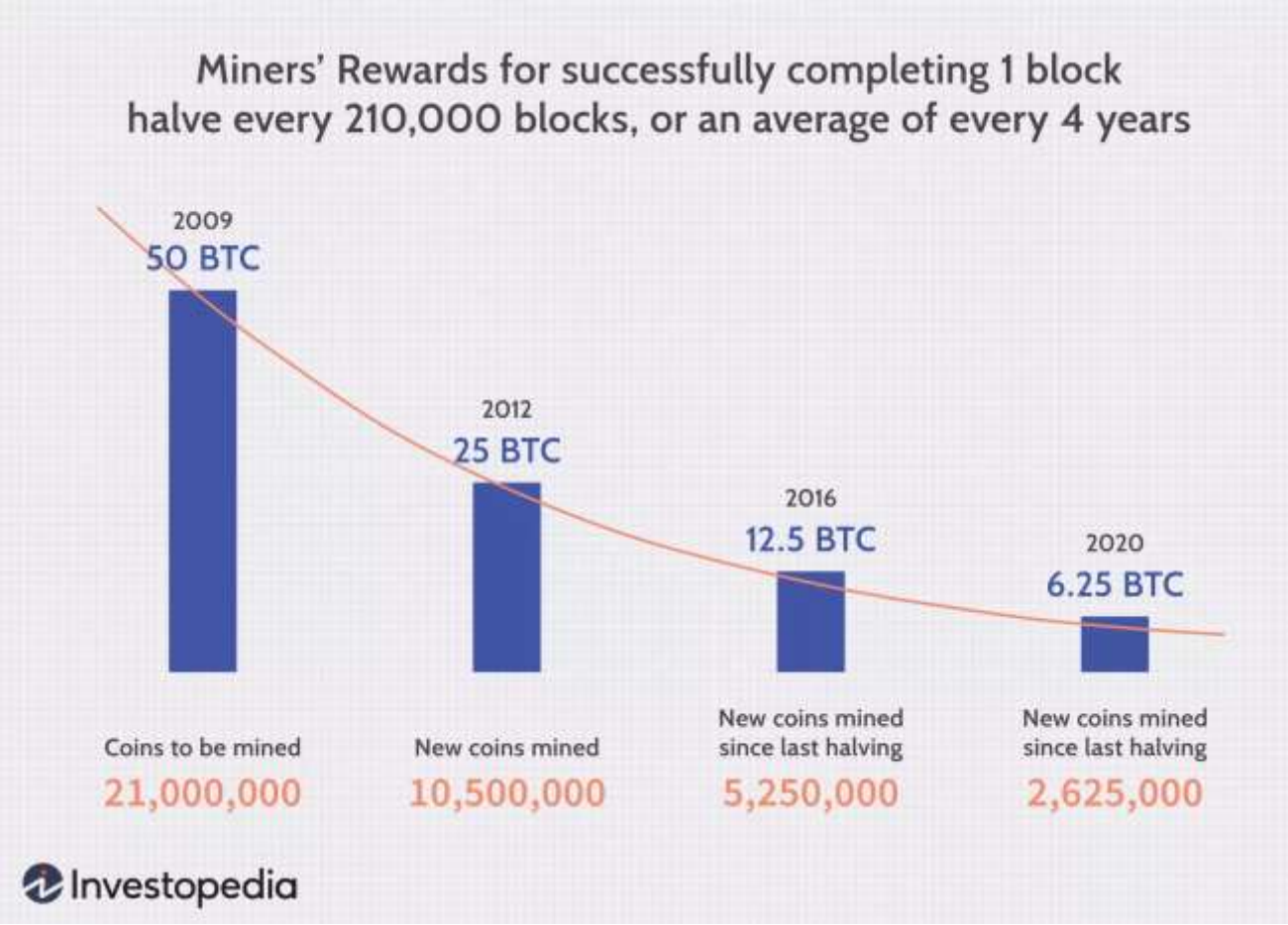
In addition to lining the pockets of miners and supporting the Bitcoin ecosystem, mining serves another vital purpose: It is the only way to release new cryptocurrency into circulation. In other words, miners are basically "minting" currency. For example, as of September 2021, there were around 18.82 million bitcoins in circulation, out of an ultimate total of 21 million.2

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 bitcoins 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. However, because the rate of bitcoin "mined" is reduced over time, the final bitcoin won't be circulated until around the year 2140. This does not mean that transactions will cease to be verified. Miners will continue to verify transactions and will be paid in fees for doing so in order to keep the integrity of Bitcoin's network.

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. This is known as a BIP (Bitcoin Improvement Protocol). In other words, miners have some degree of influence on the decision-making process on such matters as forking.

How Much a Miner Earns

The rewards for Bitcoin mining are reduced by half roughly every four years.1 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 12.5 BTC. On May 11, 2020, the reward halved again to 6.25 BTC.



In September of 2021, the price of Bitcoin was about $45,000 per bitcoin, which means you'd have earned $281,250 (6.25 x 45,000) for completing a block.4

Not a bad incentive to solve that complex hash problem detailed above, it might seem.

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 reduction of new coins entered into circulation. This lowering inflation rate increased scarcity and historically the price has risen with it.

SAINTS PERSPECTIVES
Things Scientific and Technical

What You Need to Mine Bitcoins

Although early on in Bitcoin's history individuals may have been able to compete for blocks with a regular at-home personal 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 the smooth functioning of the blockchain and its ability to process and verify transactions, 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.1

When there is more computing power collectively working to mine for bitcoins, the difficulty level of mining increases in order to keep block production at a stable rate. Less computing power means the difficulty level decreases. At today's network size, a personal computer mining for bitcoin will almost certainly find nothing.

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.

An Analogy

Say 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 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 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 or, in other words, 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"?

Here is an example of such a number:

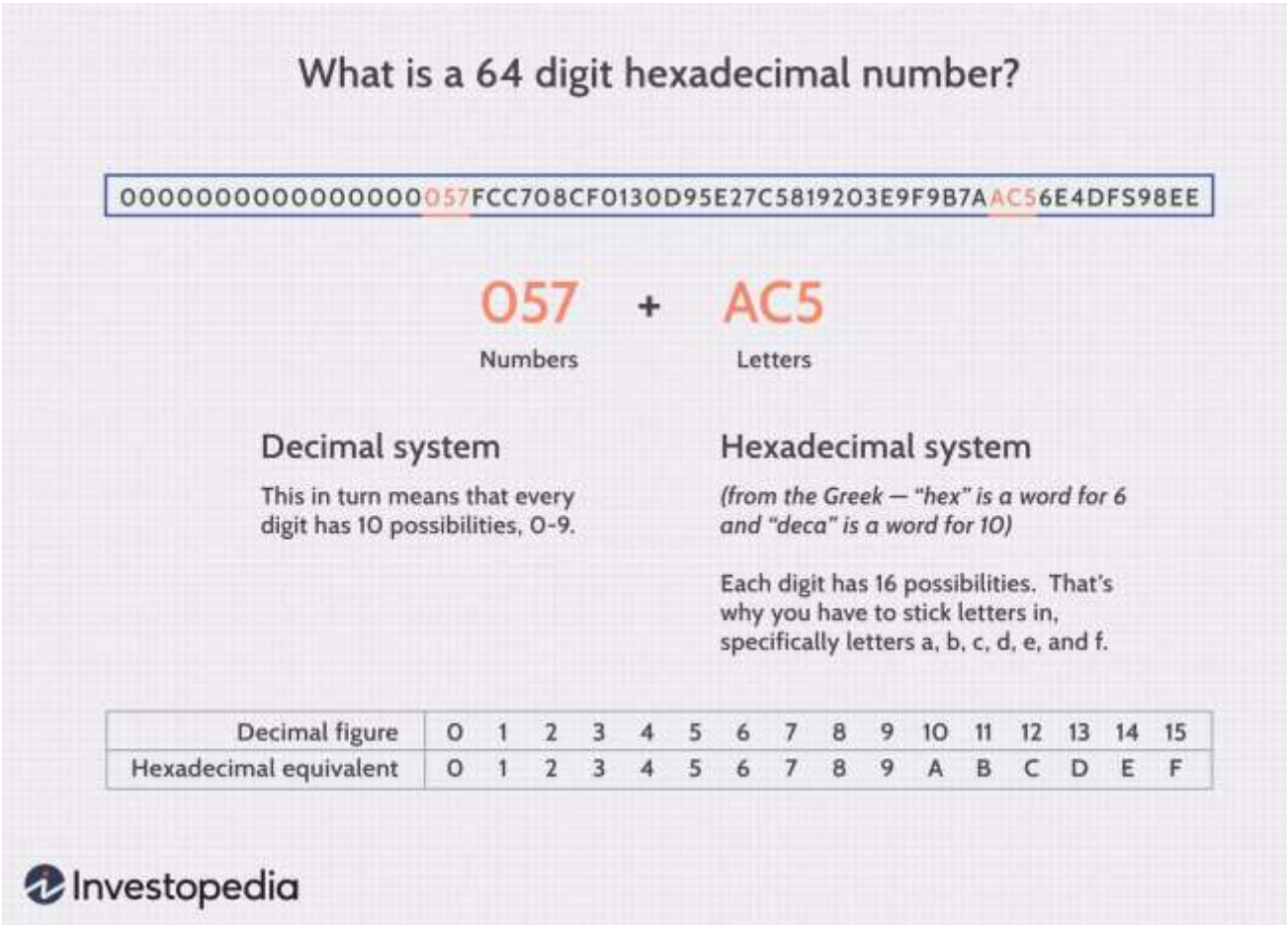
0000000000000000057fcc708cf0130d95e27c5819203e9f967ac56e4df598ee

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."

The decimal system uses as its base factors of 100 (e.g., 1% = 0.01). This, in turn, means that every digit of a multi-digit number has 100 possibilities, zero through ninety-nine. In computing, the decimal system is simplified to base 10, or zero through nine.

SAINTS PERSPECTIVES
Things Scientific and Technical



"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 analogy, where the number 19 was written 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 6.25 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."

Block #490163

Summary	
Number Of Transactions	1768
Output Total	6,903.29862618 BTC
Estimated Transaction Volume	843.56466563 BTC
Transaction Fees	1.41094004 BTC
Height	490163 (Main Chain)
Timestamp	2017-10-16 15:29:07
Received Time	2017-10-16 15:29:07
Relayed By	AntPool
Difficulty	1,196,792,694,098.79
Bits	402713392
Size	999.263 kB
Weight	3669.587 kWU
Version	0x20000000
Nonce	731511405
Block Reward	12.5 BTC

Hashes	
Hash	00000000000000000c508bc2ada8ebc62cf1c69cb66a163d9a99abad87599b6
Previous Block	0000000000000000000590d60e05a1ab8746a40b29a3c693613ddf1d5627a7ea
Next Block(s)	000000000000000060cf40270bcb84e5cb40573642d37c56d089f3148399a4

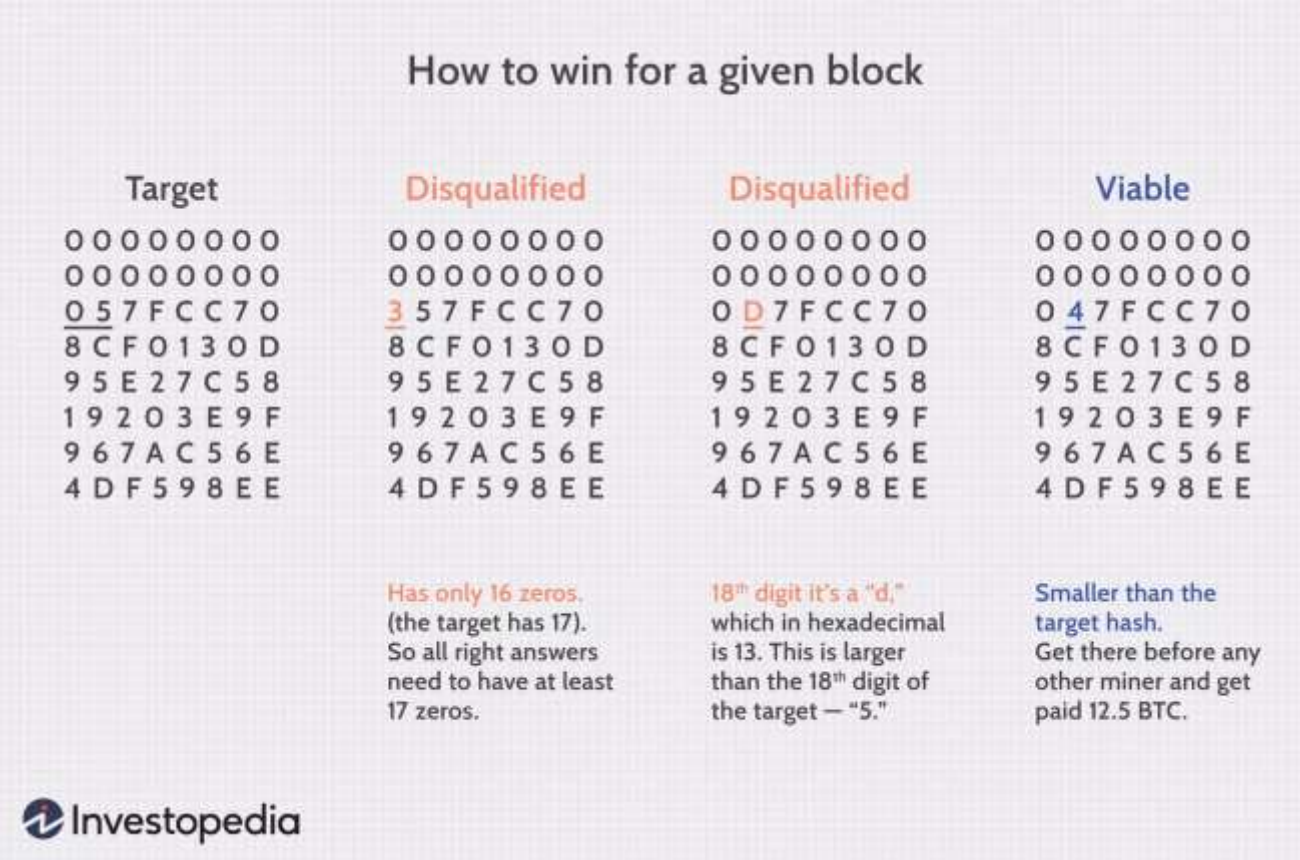
How do I guess at the target hash

All target hashes begin with a string of leading zeroes. There is no minimum target, but there is a maximum target set by the Bitcoin Protocol. No target can be greater than this number:

00000000**ffff**0000000000000000000000000000000000000000000000000000

The winning hash for a bitcoin miner is one that has at least the minimum number of leading zeroes defined the mining difficulty.

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



To find such a hash value, you 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. At today's difficulty levels, the odds of finding the winning value for a single hash is one in the tens of trillions.5 Not great odds if you're working on your own, even with a tremendously powerful mining rig.

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.

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 miners. 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 simply buy it on one of the many exchanges. 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.

To put it in modern terms, invest in the companies that manufacture those pickaxes. In a cryptocurrency context, the pickaxe equivalent would be a company that manufactures equipment used for Bitcoin mining. You may consider looking into companies that make ASICs equipment or GPUs instead, for example.

SAINTS PERSPECTIVES
Things Scientific and Technical

Downsides of Mining

The risks of mining are often that of financial risk and a regulatory one. As mentioned, Bitcoin mining, and mining in general, is a financial risk since one could go through all the effort of purchasing hundreds or thousands of dollars worth of mining equipment only to have no return on their investment. That said, this risk can be mitigated by joining mining pools. If you are considering mining and live in an area where it is prohibited you should reconsider. It may also be a good idea to research your country's regulation and overall sentiment towards cryptocurrency before investing in mining equipment.

One additional potential risk from the growth of Bitcoin mining (and other proof-of-work systems as well) is the increasing energy usage required by the computer systems running the mining algorithms. While microchip efficiency has increased dramatically for ASIC chips, the growth of the network itself is outpacing technological progress.6 As a result, there are concerns about the environmental impact and carbon footprint of Bitcoin mining.7

There are, however, efforts to mitigate this negative externality by seeking cleaner and green energy sources for mining operations (such as geothermal or solar), as well as utilizing carbon offset credits. Switching to less energy-intensive consensus mechanisms like proof-of-stake (PoS), which Ethereum has transitioned to, is another strategy; however, PoS comes with its own set of drawbacks and inefficiencies such as incentivizing hoarding instead of using coins and a risk of centralization of consensus control.

Why is it called bitcoin "mining"?

Mining is used as a metaphor for introducing new bitcoins into the system, since it requires (computational) work just as mining for gold or silver requires (physical) effort. Of course, the tokens that miners find are virtual and exist only within the digital ledger of the Bitcoin blockchain.

Why do bitcoins need to be mined?

Since they are entirely digital records, there is a risk of copying, counterfeiting, or double-spending the same coin more than once. Mining solves these problems by making it extremely expensive and resource-intensive to try to do one of these things or otherwise "hack" the network. Indeed, it is far more cost-effective to join the network as a miner than to try to undermine it.

What do you mean mining confirms transactions?

In addition to introducing new BTC into circulation, mining serves the crucial role of confirming and validating new transactions on the Bitcoin blockchain. This is important because there is no central authority such as a bank, court, government, or anything else determining which transactions are valid and which are not. Instead, the mining process achieves a decentralized consensus through proof-of-work (PoW).

Why does mining use so much electricity?

In the early days of Bitcoin, anybody could simply run a mining program from their PC or laptop. But, as the network got larger and more people became interested in mining, the difficulty of the mining algorithm became more difficult. This is because the code for Bitcoin targets finding a new block once every ten minutes, on average.1 If more miners are involved, the chances that somebody will solve the right hash quicker increases, and so the difficulty is raised to restore that 10-minute goal. Now imagine if thousands, or even millions more times of mining power joins the network. That's a lot of new machines consuming energy.

Is Bitcoin Mining Legal?

The legality of Bitcoin mining depends entirely on your geographic location. The concept of Bitcoin can threaten the dominance of fiat currencies and government control over the financial markets. For this reason, Bitcoin is completely illegal in certain places.

Bitcoin ownership and mining are legal in more countries than not. Some examples of places where it was illegal according to a 2018 report were Algeria, Egypt, Morocco, Bolivia, Ecuador, Nepal, and Pakistan.8 Overall, Bitcoin use and mining remain legal across much of the globe.

Addendum

Opinion of someone into Cryptocurrencies

In many respects **Proof of Work** mining used by Bitcoin has a ‘chance of winning’ component (like a lottery) but as the article explains, the main purpose of mining is (1) to incentivise people to run the distributed ledger which validates transactions and (2) a mechanism to generate new currency.

As noted in the article, Proof of Work mining has a specific downside of consuming a lot of energy with these miners trying to guess the target hash. Unfortunately for Bitcoin it is stuck with this model for the foreseeable future. The **'crypto community'** however found a solution to this problem which does not involve a lot of computing power guessing… its the “**Proof of Stake”** model https://www. which is being used by the newer crypto currencies (**Cardano, Polkadot, Solana, Algorand, and soon ETH2.0**).

In **Proof of Stake**, the two problems noted above (running the ledgers to validate transactions and generating currency) are solved by the ‘put your money where your mouth is’ approach.
As an example, Solana is a relatively new cryptocurrency that I bought 10 SOL tokens last summer. I proceeded to ’stake’ them with a Validator https://stake.fish/en/solana/

In this model, there is no 'mining' per se… the big downside to this is the system needs to be truly decentralised to be safe… right now Solana only has 1200 Validator pools. Of these, 41 pools own more than 50% of staked SOL tokens https://solanabeach.io/ …. If these 41 entities get together or were bought out by some big single entity they could agree to change the ledger to whatever they wanted which would probably crash the price. For now however this is fairly low risk.

One other point… with this **Proof of Stake model**, there is not much computing power needed to be a Validator. This task can be run on a **Raspberry Pi machine** (see here as example) … I think you can agree this is a smarter solution and why with all these smart people working on this new technology, Cryptocurrencies are here to stay.

Related Articles:

<TBD>