Introduction to Bitcoin Mining

A Guide For Gamers, Geeks, and Everyone Else

by

David R. Sterry

If you find this eBook useful and would like to see it extended, send donations to 1i2mRogbNByFLxuhD7HtjxDut8GDPnmYj

For the most recent version please visit CoinDL.com

Contents

Introduction

A thousand men, say, go searchin' for gold. After six months, one of them's lucky: one out of a thousand. His find represents not only his own labor, but that of nine hundred and ninety-nine others to boot. That's six thousand months, five hundred years, scramblin' over a mountain, goin' hungry and thirsty. An ounce of gold, mister, is worth what it is because of the human labor that went into the findin' and the gettin' of it.

– Howard, The Treasure of the Sierra Madre (1948)

So you fancy yourself a Bitcoin miner. Or maybe you just want more insight into the most amazing technological development since the wheel. Either way, *Introduction to Bitcoin Mining* will get you started right.

While mining can be as challenging as you make it, this guide will help you take the first steps. Whether you're interested in using the hardware you have or if you are planning to upgrade, you will find *Introduction to Bitcoin Mining* a helpful resource as you mine your first coins.

Bitcoin is unlike anything the world has seen before. By providing fast, inexpensive, international money transfer, it has the potential to revolutionize both the modern day concept of money and commerce. Bitcoin started as a free software project and a paper published by Satoshi Nakamoto in 2009. Nakamoto, who seems to have been created specifically to deliver Bitcoin to this world, designed a system of online value transfer that supports a promising Internet currency.

Bitcoin is made possible by a combination of software and network technologies. A program called the Bitcoin client simultaneously manages and helps you spend bitcoins. This program maintains a long ledger called the blockchain that holds every transaction confirmed by the Bitcoin network.

The Bitcoin network, consisting of thousands of machines running the Bitcoin software, has two main tasks to accomplish. One is relaying transaction information and the second is verifying those transactions to ensure the same bitcoins cannot be spent twice.

The first task is accomplished easily due to the fact that the Bitcoin network is operated as a peer-to-peer network. After all, sharing data is easy. By operating on many nodes across the globe, the network ensures it will operate as long as it provides a useful service.

The second task is a bit more complicated and is solved through what I consider to be Bitcoin's key innovation. This development, a process called mining, is carried out by computers running mining software.

The rest of this handbook will cover the reasons for mining, the hardware and software you will use, mining alone as well as in pools, optimizing techniques, and will finish with information on safely using and storing bitcoins.

Why Start Mining?

Reasons to mine are numerous and varied. Your reasons may change over time as you learn about Bitcoin and follow its progress. It is helpful to understand others' motivations to be able to trust the Bitcoin network and the currency it supports.

Many people get started mining by a natural extension of something else they are already doing. For example, Bitcoin mining is similar to other grid computing projects that have grown because they are fun and provide an opportunity to cooperate with others in solving a big problem.

In the case of Folding@Home, a distributed-computing project focused on studying protein folding, users contribute their computer processing power to increase scientists ability to understand how proteins fold. Donors and teams compete and cooperate to see who can help the project the most. By mining bitcoins, you help to solve the problem of creating a currency and payment network that does not rely on a central issuing authority.

Those who are involved in technology are used to constant innovation and realize it is important to stay informed as new technologies emerge. Bitcoin is a new combination of several novel technologies(cryptography, peer-to-peer networks, distributed databases) and some users mine bitcoins to help build experience with these technologies.

Since Bitcoin functions as a currency and mining can be operated as a business process, a large number of miners do it for profit. It is a tough business however because Bitcoin prices can fluctuate fairly widely and investment costs for a mining business can easily be in the tens of thousands of dollars. If you can operate efficiently, you may want to attempt to mine for profit but be sure to do your homework before making any big purchases.

Mining is a way to get bitcoins and this appeals to those who might want to obtain bitcoins steadily without using services such as exchanges or by selling any good they produce or service they perform as a profession.

Another motivation may be for anonymity. If you solve a block and are careful to connect to the Bitcoin network using Tor (The Onion Router), mining is a way to obtain bitcoins completely anonymously.

In addition to being a payment network, Bitcoin is a software project and there are many software projects that depend on the Bitcoin network for their own success. If your project depends on Bitcoin, you may want to contribute some hashing power to the network to increase, even in some small way, the chance of success.

There are probably more reasons still but the final reason we'll list here to mine bitcoins is if you depend on the Bitcoin network for international commerce and wish to see it as strong as possible.

What Is Mining?

Bitcoin is really three things. First it is a protocol (or set of rules) that defines how the network should operate. Second it is a software project that implements that protocol. Third it is a network of computers and devices running software that uses to protocol to create and manage the Bitcoin currency.

Mining is defined in the protocol, implemented in software, and is an essential function in managing the Bitcoin network. Mining verifies transactions, prevents double-spending, collects transaction fees and creates the money supply. Mining also protects the network by piling tons of processing power on top of past transactions.

Mining verifies transactions by evaluating them against the transactions that happened before. Transactions cannot spend bitcoins that do not exist or that were spent before. They must send bitcoins to valid addresses and adhere to every rule defined by the protocol.

With a frequency that is targeted at every 10 minutes, mining creates new blocks from the latest transactions and produces the amount of bitcoins defined by the current block reward (50 BTC until late 2012). Miners also verify blocks produced by other miners to allow the entire network to continue building on the blockchain.

Finding Valid Blocks

To find a valid block, the miner builds a list of recent transactions and calculates some summary information about the proposed block. This summary is combined with a number called a nonce to create a block header. The hash of the block header is then calculated and to see if it is small enough to win at the current difficulty. If not, the nonce is changed and the new hash is calculated and tested.

There is no way to create a valid block except by a brute force search. Brute force means the miner tries one nonce, then another, and another, repeating the process until it gets lucky. During that search, the miner cannot predict if the next nonce will give a smaller hash than the last.

Since it is a brute force process, the only way to increase your chances of winning are to increase the speed with which you can try nonces. The more processing power you have at your disposal, the faster you can search and the more likely you will be to find a winning block.

Once a valid block has been generated, it is broadcast to the network and quickly verified by the other nodes in the network. The difficulty of finding a winning number is adjusted every 2016 blocks so blocks are generated on average, every 10 minutes.

Creating New Bitcoins

When a miner finds a new block, it includes a new address to which new bitcoins and any transaction fees are to be awarded. This reward is the monetary incentive for people like you and me to run miners. If the conditions are right, you can put mining hardware to work, paying for your time and electricity and make a profit by selling the resulting bitcoins that you were awarded.

As this guide is being written, 50 bitcoins are awarded to the miner who finds each block. This will continue until block 210,000 is found at which time the block reward will halve to 25 bitcoins. The reward will then halve again every 210,000 blocks thereafter. This means the number of Bitcoins ever created will top out at around 21 million (estimated to occur in near 2040).

Where do these bitcoins come from? They are literally created by the network as part of the Bitcoin protocol. This is the same process that created any bitcoins you will ever own or use.

Mining Hardware

Above, I used the term miner to describe a person who sets up mining computers, the computer hardware doing the mining, or the software that executes the logic required in mining. Hardware is the focus of this section.

As you know, some computers are faster than others. Computers can have faster or slower processors, more or less RAM, bigger and smaller hard drives, and so on. It is also true that some types of processor are better at mining than others. Since the testing of nonces is a very repetitive task, computer hardware that does repetitive things quickly works best for mining.

What is commonly referred to as the processor in a computer (the CPU) is a processor that is very good at switching tasks. Its parts are arranged in a way that helps the computer switch from playing video to messaging someone or showing a PDF. The CPU is optimized for task switching since that is how it spends most of its time.

On the other hand, a computer's GPU (graphics processing unit) is called upon to do simple operations, like draw a triangle, or shade a pixel, as many times per second as possible. It is internally arranged for this purpose which makes it much faster and more efficient for Bitcoin mining. In fact, we find that common video cards can out-perform common CPUs by 100x or more. Since you are competing with other miners, mining with anything less powerful than the top 10 or 20 video cards is quite inefficient.

The most recent development in Bitcoin mining is another processor called the FPGA (Field Programmable Gate Array). An FPGA is simply a highly programmable processor. FPGAs tend to be more expensive than CPUs and GPUs but they are also quite efficient in their use of electricity. Miners who are looking to operate where electricty is more expensive can invest more money up front to buy an FPGA miner and then pay less in ongoing electricity costs.

Mining Software

If you're mining with a GPU, you will need software to direct the hardware to mine Bitcoins. Software is available for Windows, Mac, and GNU/Linux. Much of this software is free and open source software that you can download and setup yourself or with a little help from someone online.

Once you have the software running, it will tell you how quickly it is mining. This is a number denoted in hashes per second with common speeds today in the mega-hashes or giga-hashes per second. A hash is a step toward testing a nonce and mega and giga mean million and billion respectively.

The goal is to get as many hashes completed by your hardware as possible per unit time. The best software for your hardware will help you do that. Good software gives a good hash rate but is also stable, meaning mining doesn't stop because of a glitch in the software.

After you've chosen mining software, there may also be specific settings you will use when you start the miner. These settings, which vary too much from machine to machine to list here, will help to obtain maximum performance from your miner. You can find settings for your GPU on the bitcoin wiki and forums.

Running your miner

When you're ready to mine, you'll start your miner. This may involve starting the same program multiple times if you have multiple GPUs or you may choose to use software that runs as a Live CD or Live USB boot disk that will take over the entire computer and manage the mining for you.

You'll want to check on your miner from time to time to be sure it is running and getting a good hash rate. This especially the case if you've done some of the more exotic tweaks to maximize your hashes per second. There are mobile apps and websites that can help you stay updated as to the status of your miner.

When you win a block(we'll get to mining pools soon), your bitcoin balance will increase by the amount of the block reward plus the transaction fees that were paid with any included transactions.

Running Multiple Miners

If you are inclined to invest more hardware and resources into mining bitcoins, is is possible to connect multiple miners together on a network. To do this, you'll need some basic network equipment like a router and a computer to run bitcoind (the bitcoin daemon). You'll need to setup a user and password so the miners can all talk to the running instance of bitcoind. When a block is found by one of your miners, your bitcoind will contain the wallet with the key that signs the block and claims the block reward and fees.

Running multiple miners has power and heat implications that you'll want to consider. A high-end mining computer can use as much power as a toaster, iron or vacuum cleaner so if a circuit breaker trips you'll want to re-evaluate how your power is distributed on your wiring.

In regards to generated heat, this may be a nice byproduct on a cold winter night but on a hot day you'll want to have a way to remove heat from your space.

Overclocking

Computer processors have a speed at which they run called the clock speed. For modern processors this is stated in gigahertz. After a processor is manufactured it is tested to see how fast of a clock speed it can reliably support. Chips that are not stable at higher clock speeds are sold as lower speed models. Adventurous computer users have, for many years, been squeezing out more power from their processors by increasing the clock speed - a technique called overclocking.

GPUs generally have a software tool that is used to change the clock speed of the processor as desired. GPUs also have a RAM clock speed that can be adjusted.

As we said before the goal is to get as many hashes calculated as possible per unit time. We want to get a high hashrate but we also want stability. The problem with overclocking is that there is a limit to how much you can overclock your GPU without causing your miner to lock up or freeze. When locked up or frozen, the hash rate will drop to 0 or, in the case of a multi-GPU setup, a fraction of what it would be normally.

You'll need to experiment with your hardware to find out what gives the best, most consistent clock rate.

In regards to GPU RAM clock speed, this is often reduced in order to save electricity and help video cards run cooler at a given clock speed and resulting hash rate.

Solo Mining

Mining is a chance endeavor and the probability of winning a block within a given period of time can be calculated. Unfortunately for many systems, the time required to have a good chance at mining a block can be in the months or years.

If you have several machines running at high hash rates, you will find blocks more often and may be able to absorb the variation in the rate at which blocks are mined. On the other hand if you're running with a lower hash rate and can stand running longer in hopes of getting lucky, solo mining can still make sense. If you would prefer more certainty and evenness of payouts, you will want to mine in a pool which will be covered in the next section.

Pooled Mining

Winning a block will most likely be quite infrequent so mining pools were created as a way to even out the rewards. Those who join a mining pool cooperate to mine blocks as a group and when a block is solved by one of the members, the rewards are shared.

The amount going to each contributor takes into account their hashrate and time mining for the pool. Mining pool operators may take a percentage of the Bitcoins as payment for creating and running the pool. There are many pools to choose from and mining clients can be easily switched from one pool to another.

It is a good idea to join at least two pools in case the first one becomes unavailable for some period of time. Without a backup pool, your hashrate will effectively drop to zero until your pool becomes available again.

Managing Your Bitcoins

Whether you're mining solo or as part of a pool, with one computer or with many, eventually you will have some bitcoins. Once you get them it is important to handle them properly. Let's go over the wallet and how your Bitcoins are stored in practice.

When you run a Bitcoin client for the first time, it creates a Bitcoin wallet. The wallet contains your private keys, made of long blocks of random letters and numbers, that are meant to be kept secret. These keys are what allows your Bitcoin client to spend and, you to effectively own, your bitcoins.

From each private key, a public key and corresponding Bitcoin address are created. When someone sends you some bitcoins, their Bitcoin client uses their private key to sign the bitcoins over to one of your addresses. This transaction is broadcast to the bitcoin network and later recorded in a block.

The important point to know here is that bitcoins aren't actually sent anywhere. They are instead assigned to addresses. To send bitcoins to yet another address the private key of the address that owns them will be required. This means you need to secure and backup your wallet to protect it against theft, virus attack, or loss due to hard drive failure or natural disaster.

The simplest way to backup your wallet is to use the backup feature of your Bitcoin program. If no such facility exists or you would like an additional backkup, find your Bitcoin configuration folder and make a full backup of it. Be sure to have turned off your Bitcoin program however before making this copy.

Place this backup on one or more flash drives or CDs and put those somewhere safe. Depending on the number of Bitcoins you have, you may want to keep your backups in a safe or safe deposit box until they need to be used.

In regards to backup, it is a good idea to test the backup on another secure system. It is said that you do backup but what you really want is restore. So test your backups. Just be sure to test it on another system because some people have lost bitcoins by restoring a backup over a wallet that had private keys that were not in the backup.

Next is protection from online threats. This means keeping the wallet either offline or on a computer that is disconnected from the internet. If you'd like to have reasonable yet secure access to your Bitcoin wallet you can use a live CD with your computer to access and manipulate your bitcoins. The live CD would include all the software needed to handle bitcoins.

If you're going to be placing your backups where other people may be able to access them, you can use encryption. Once encrypted, a potential thief would need your password to be able to access the wallet file and steal your bitcoins. As an example, and there are many, a program like Truecrypt provides a simple way to encrypt one or more files on any drive or computer you wish. The latest version of the Bitcoin program from bitcoin.org also includes wallet encryption.

Using Bitcoins

Bitcoins are money and can be used as such. You can send them to friends to settle small debts. You can sell something or work for bitcoins. You can also buy products and services online with them. Currently there are hundreds of business that accept Bitcoin online and around the globe.

For business that only accept dollars, Euros, yen and other national currencies you will need to exchange your bitcoins. This can be done on one of the many online Bitcoin exchanges or by finding someone local who will to buy them from you.

To sell bitcoins on an exchange you would create an account with the exchange, send them your Bitcoins and place an order to sell. Then when a corresponding buy order appears, your bitcoins will be traded for the currency you prefer. Then you'll need to get your money sent to you via a money transfer method that is compatible with Bitcoin.

One very important feature of Bitcoin is irreversibility. Once bitcoins are sent to an address, there is virtually no way to reverse the transaction. I hesitate to even say virtually because doing so requires either extremely fast timing or government-sized mining power. No credit card company or bank can get them back. The mathematics behind Bitcoin are very strong.

Bitcoin is therefore incompatible with financial services that allow payments to be disputed or "charged back". Notable examples include PayPal, credit card, check, and ACH. In the economy that grows around Bitcoin, refunds will need to be performed by the receiver of the funds and buyers will be wise to use escrow services with vendors they do not trust.

Accounting

At this time there isn't much in the way of Bitcoin portfolio tracking or Bitcoin-based accounting software. It is wise however until something good comes along, to save records of all your transactions. You will want to know how many bitcoins you have, how you got them, and in which wallets they are stored.

Conclusion

Bitcoin is a new Internet currency that anyone can get started mining. There are a number of reasons you might mine: for profit, to help secure the network, to help found a new Internet currency, or just to gain technical experience. Hopefully *Introduction to Bitcoin Mining* has proved informative and helps you get started mining!

If you have any comments, questions or suggestions please email davids@exchb.com.

Further reading / Online resources

Mining Hardware Comparison:

https://en.bitcoin.it/wiki/Mining_hardware_comparison

Securing Your Wallet: https://en.bitcoin.it/wiki/Securing_your_wallet

Updated Bitcoin Information: http://www.weusecoins.com/

Official Bitcoin Forums: https://bitcointalk.org/

Bitcoin Market Charts: http://bitcoincharts.com/

Bitcoin Exchange Rate and Converter:

http://bitcoinexchangerate.org/