How to Mine Bitcoins

What is Bitcoin mining

Bitcoin transactions are registered in a public ledger called block chain. This chain is composed of blocks containing one or more transactions. In order to register a transaction, it has to be previously verified. The process of verifying and registering a Bitcoin transaction is called Bitcoin mining. The process also includes a reward for the miners in the form of Bitcoins.

How is the process

Since Bitcoins are a digital currency, there is the risk that someone makes a copy of a Bitcoin and tries to spend it. This is called the double spending problem.

Bitcoins solve this problem by making all transaction public and storing them in a distributed database named Blockchain. These two features ensure transparency and accountability.

The people who confirm and store the transactions are called “miners”. They register the transactions in blocks. The records contain information about the transaction and a number called “nonce”. The information cannot be changed. However, the nonce can be changed, and is used to create a reward for the miners in the form of Bitcoins.

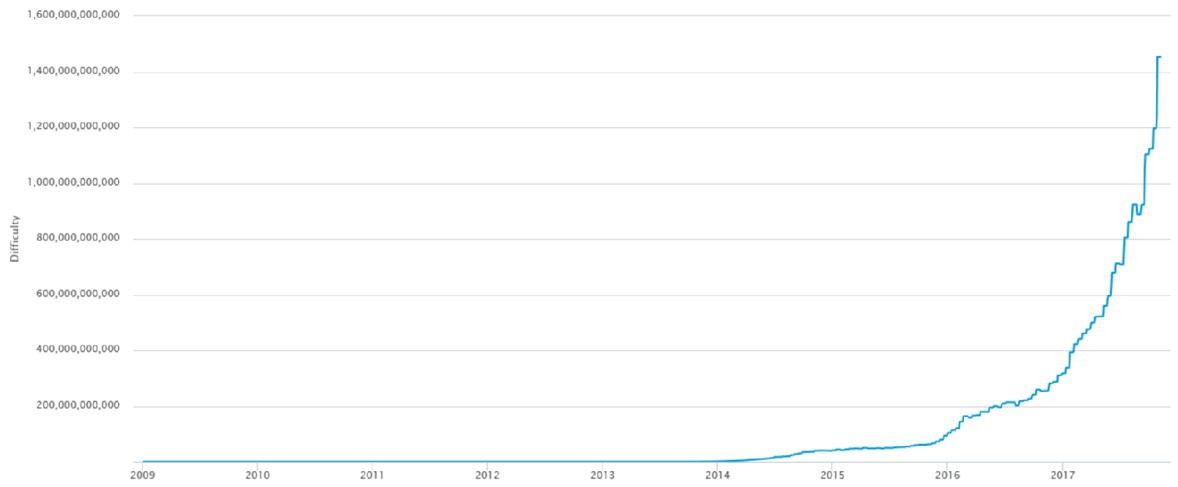
In order to obtain the reward, miners create a Hash with the nonce by using the SHA-256 algorithm. But, there is a condition: the Hash must contain a number of predefined zeros. The amount of zeros defines the difficulty of the problem.

The first one to solve the puzzle gets the proof of work and the reward, and broadcasts the block to all nodes. The other nodes accept the block only if all transactions contained in it are valid, and the Bitcoins have not been previously spent.

The acceptance is confirmed by creating a new block with the accepted Hash as the previous Hash.

Difficulty of the puzzle and the reward

In order to keep the number of blocks found per day constant, the difficulty of the problem is increased every two weeks. In addition, the amount of Bitcoins in the reward is halved every four years.



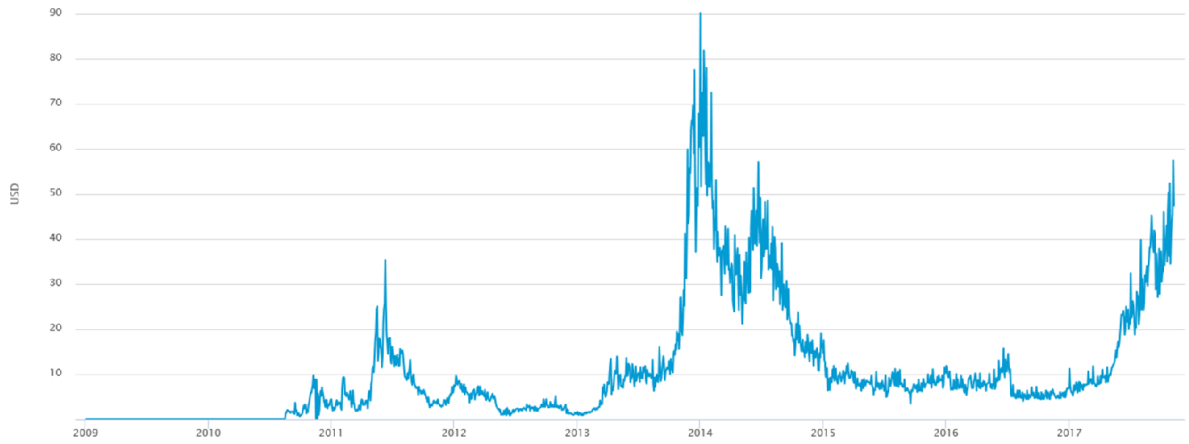
Difficulty

Source: https://blockchain.info/charts/difficulty Retrieved on the 8th November, 2017.

This keeps the amount of blocks found at approximately one every ten minutes, and a possible maximum of 21 million Bitcoins. In the beginning, the reward consisted of 50 Bitcoins. At present it is 25 Bitcoins.

Hardware resources

In the beginning, miners used computers with average CPUs. As the complexity of the mining process increased, miners started to use computers with Graphical Processing Units (GPUs).



Cost-per-transaction

Source: https://blockchain.info/charts/cost-per-transaction Retrieved on the 8th November, 2017.

In 2011, the mining industry got more complex, and special mining devices were introduced. These devices were based on Field-programmable Gate Array (FPGP) processors and connected to a computer via a USB.

Because these devices consumed much less resources, they allowed for the creation of the first mining farms.

Today, mining is done with Application-specific Integrated Circuits (ASIC). Several of these products are available on the market.

ASIC chips are specifically created to solve Bitcoin blocks. During these past years, as more people entered into the mining race, the sophistication of these devices has increased. Some well know Bitcoin miners include Antminer S5, Antminer U3, ASICMiner BE Tube, ASICMiner BE Prisma, Avalon 2, Avalon 3, and BTC Garden AM-V1 616 GH/s.

Mining farms

One of the largest Bitcoin farms is located in Ordos, Inner Mongolia, China. The city is a former industrial place, with cheap access to power and several semi-finished buildings, where over 25000 machines are doing the calculations necessary to solve the Bitcoin puzzles. It belongs to a company named Bitmain.

The Ordos mining farm is a typical example of a mining farm. With increasing difficulties in the mining process, and an ever increasing competition, the lone mining machine is not possible any more. In addition, with the high value of Bitcoins, profits from these farms can be in the millions of dollars. Today, with its entrepreneurial spirit, China is one of the most important Bitcoin mining countries in the world.

Miners' revenue

Source: https://blockchain.info/charts/miners-revenue Retrieved on the 8th November, 2017.

Mining pools

When you don't have enough recourses by yourself, you can still mine by participating in a mining pool.

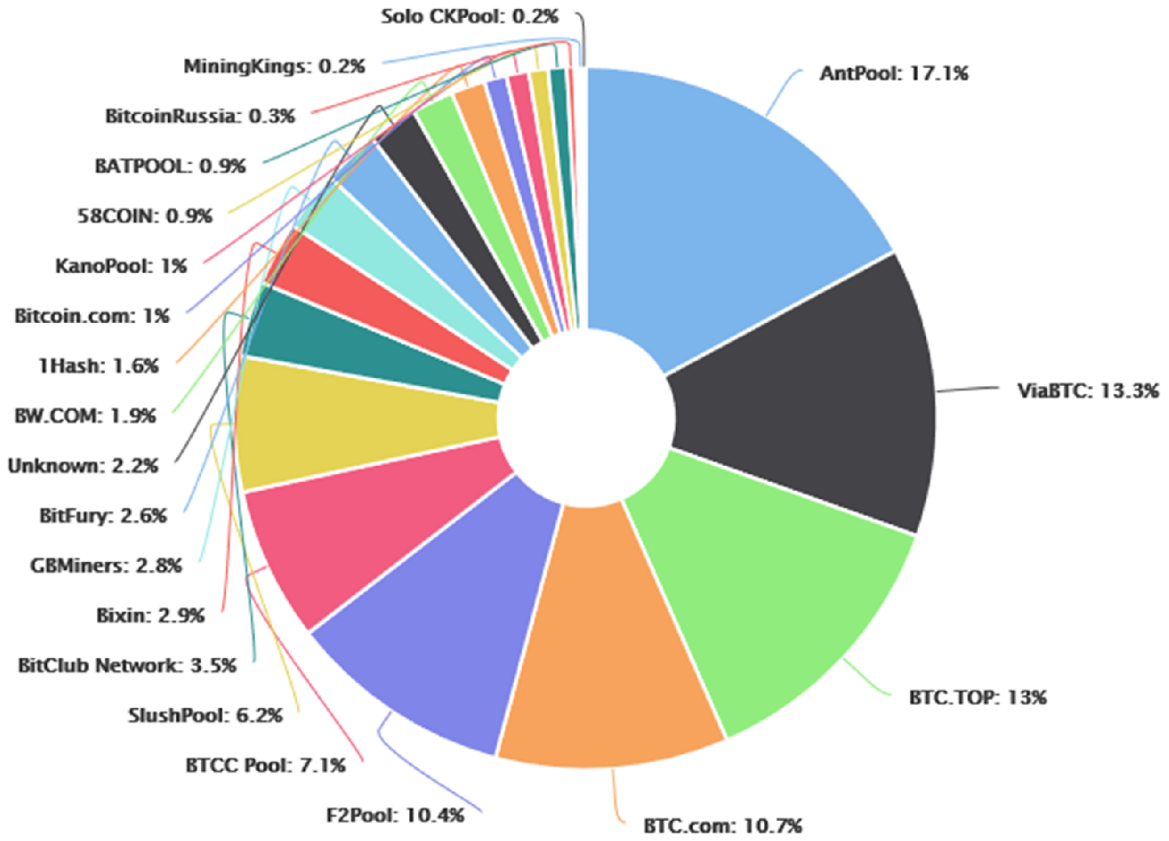
These are groups of miners, who cooperate and share the reward, usually in proportion to their contribution to the total hash mining power.

They started when mining became too sophisticated, to the point that it would take years for a lone miner to solve the puzzle.

However, they have the disadvantage that they are controlled by the pool owner. China has a big concentration of mining pools. The figure below shows the main mining pools during 4 days in November 2017.

Some of the best known mining pools are:

- Antpool, which is based in China and owned by BitMain. The website is https://www.antpool.com/
- BTC.top, which is private and closed to the public. The website is http://btc.top/ , and it is available only in Chinese.
- BTC.com, which is open to the public; BTCC, which is also based in China. The website is https://btc.com/
- Slush Pool, which is owned by Satoshi Labs and based in the Check Republic. It was the first mining pool. The website is https://slushpool.com/home/
- Eligius, which was created by Luke Dashjr, a Bitcoin Core developer. The website is http://eligius.st/index.php/~gateway/
- F2Pool, which is only available in Chinese. The website is https://www.f2pool.com/
- Bitfury, which is private and not open to the public. The website is http://bitfury.com/



Pools and Hashrate distribution (last 4 days)

Source: https://blockchain.info/pools Retrieved on the 8th November, 2017.

Cloud Services

For those not interested in having their own devices, there are some cloud based contract services. However, there have been many scams in this area. Some well-known cloud mining services are Hashflare, Hashing 24 and Genesis Mining. However, it should be noted that this article only mentions product names; it doesn't recommend any of them in particular.

Wrapping up

Bitcoin mining is the process used to record transactions in the public ledger. The process presents a puzzle and a reward for those who solve the puzzle. At present the sophistication of the problem implies that huge resources are needed. This fact has prompted the creation of cloud services, mining farms and mining pools. If you want to be part of the race, you need to join one of them to be able to profit.