**WHAT IS MINING - HOW IT WORKS**

One of the issues, which has more relevance in the Blockchain world, and specifically Bitcoin, is the cryptocurrency mining. In this article, we will see, what is the mining, how it works, and if it is profitable today.

1. ***MINING BITCOINS***

In any traditional monetary system, governments just print more money when they need it.

Thousands of computers around the world "mine" bitcoins competing with each other.

The miners get the bitcoins as a reward for the resolution of mathematical problems in which every 10 minutes compete thousands of nodes being the most powerful computer network that exists today (Above even NSA or Google).

This mathematical challenge is always the same in its process, but the variables are different and can only be solved by trying random numbers without stopping until finding the result that is sought at that moment.

**The first one who gets it gets the reward.** This action generates competition and searches for efficiency by improving computers for this purpose, which they call miners.

1. ***HOW MINING WORKS***

People continuously send bitcoins from one place to another, but unless someone recorded all these transactions, no one could check who paid what at a certain time.

The Bitcoin network manages this by recording all the transactions carried out in a given period in a list, called a block. **The work of the miners is to confirm those transactions and write them in the "ledger"** (*chain of blocks*).

1. ***WHAT IS HASH***

**The Ledger is a long list of blocks known as the "blockchain".**

It can be used to explore any transaction that has taken place between bitcoin addresses anywhere.

Each time a new block is created, it is added to the chain, creating a growing list of all the transactions that have been made throughout the history of the Bitcoin network.

An updated real-time copy of the blocks is downloaded to each computer or node that is contributing computational power to the network.

The Ledger has to generate trust, and all this is sustained digitally.   
  
***How can we make sure that the chain of blocks remains intact and nobody manipulates it?***

This is where the miners come into play, when a block of transactions is created, the miners give rise to it following a process, they take the information from the block and apply a mathematical formula, turning it into something different.

This new "piece of information" is shorter and in appearance is a sequence of numbers and random letters technically called "Hash".

The Hash is stored with the block, at the end of it, last in the chain at that moment.

*The Hash has some interesting properties. It is easy to produce a hash of a data set as a block of transactions, but it is practically impossible to access the data simply with the has".*

While it is effortless to produce a hash of a large data set, each one is unique.

*If you change a single character of the block, the "hash" will change completely.*

The miners not only use the transactions of a block to generate a "hash". Other data are also used. One of these data is the hash of the last block added to the chain.

Because the hash of each block is produced using the hash of the immediately preceding block, it becomes a digital version of a "seal of sealing."

Confirm that this block and everyone that follows is legitimate.

If you try to fake a transaction by changing a block that has already been stored in the chain, the hash of that block will change.

If someone checked the authenticity of the block by applying the mathematical function above, they would find that the hash would be different from the one that is already stored with that block in the chain and, as a consequence, the block would be automatically identified as false.

1. ***THE RACE FOR THE COINS***

In this way the miners "seal" the blocks. Everyone competes with each other to do this, using software written specifically for mine blocks.

Each time someone successfully creates a hash, a reward of 25 bitcoins is carried, the chain of blocks is updated, and everyone in the network is notified accordingly.

That is the incentive to keep mining and allow transactions to continue to be carried out.

The problem is that it is very easy to produce a hash directly from a data set.

Since for a computer it is effortless to do this, the Bitcoin network has to make it more difficult, since otherwise, everyone would be creating "hashes" of hundreds of transaction blocks every second and all the bitcoins would be mined in minutes.

The Bitcoin protocol simply would not accept any old hash. Requires that the "hash" of each block be in a certain way, having to have some zeros determined at the beginning.

There is no way to know how a hash will be before producing it and, as soon as a new datum is included, the hash will be different.

It is assumed that the miners do not interact with the data referring to transactions that are inside each block, but they must change the data they are using to create a different hash.

They do this using another piece of random information that is known as nonce, which is used with the transaction data to create a hash.

If the hash does not conform to the required format, the "nonce" is changed and tested again by creating a new hash still.

It can take several attempts to find a nonce that works and all the miners in the network are trying to do it at the same time. In fact, it takes millions of attempts, by thousands of computers that all try to find the number that returns the pattern that is being asked at that moment.

This is the way how the miners earn their livelihood.

1. ***IT IS PROFITABLE MINING BITCOINS TODAY?***

**"Mining bitcoins is no longer profitable, but with Ethereum or other Altcoins there is an opportunity."**

Is it lthis statement true? Is it profitable today to devote to mining one of these Cryptocurrencies?  
  
We can use our home computer, although the power that we will achieve (and therefore the possibility of obtaining a return) will increase as we add powerful graphics cards or directly plates designed to mine. To calculate mining costs and profitability we have to take into account several aspects:

* *Price of electricity.*
* *Price of the components that we buy for it.*
* *Duration of those components before they become obsolete.*
* *Amount to which we can sell them once they become obsolete.*
* *Hash rate that we can get with those components. That is, the power necessary for mining.*
* *And of course, the monetary value of the cryptocurrency in question.*

Mining bitcoins at the domestic level has not been profitable or viable for years. At the end of the last decade, mining began at a private level, with home computers. Soon, many started to invest in buying more and better graphics cards until having several plates and GPUs for this activity, thus increasing the difficulty of mining.

That difficulty is given by the hash rate: the amount of hash that we can calculate per second. A hash is a number obtained from another initial number performing calculations. The first one that gets a hash that meets specific requirements receives the reward.   
  
If the time it takes to achieve is less than the fixed time, the difficulty automatically increases. And vice versa, if it takes more time than stipulated, the challenge goes down.

As the mining involves the introduction of random numbers to perform these calculations, the higher the number of calculations per second, the more likely we are to get it right, and therefore, to get the reward. That is why the increasing resources destined for mining caused the hash rate to skyrocket.

Mining bitcoins, privately, with tools and essential equipment does not come out profitable today. To mine, we should create a miner's farm, and devote a substantial investment to the same. But, also appears the opportunity to mine other currencies, in which if the mining of them can be profitable.