**¿HOW DO BLOCKCHAIN TECHNOLOGY WORKS?**

**HOW IT WORKS?**

Until now, we had always needed a third party in which both sides would trust to guarantee the authenticity of the transactions, be it a bank, an auditor, a notary or Paypal, for example, that had a record or seal of truthfulness.

The Blockchain solves this double-spending problem by combining the P2P technology of peer-to-peer exchange with cryptography and thus creating a new form of communication and digital exchange.

The transactions included in the blocks are created by the members of the system. All sales are recorded and transmitted to all nodes in the network. Thus, all members have updated information continuously with all transactions.

A node is a computer connected to the network that uses software to store and distribute an updated copy of the chain of blocks in real time.

Imagine for a moment that the network disappeared, if that happened, Bitcoin would cease to exist, that is why the Blockchain is spoken of as the genuinely revolutionary advance that lives in each of the nodes that form the network, giving rise to an extremely robust system. It is enough that there is a functioning node so that the entire network works and can be recovered in case of any eventuality.

Transactions are made from electronic wallets or wallets, which are encrypted files that work similar to a bank account. All wallets have a public key and a private key. The public key is an alphanumeric string between 26 and 35 characters. This is the Bitcoin address and acts as an account number. In this way, for someone to send you bitcoins and reach you, you must previously give them the public key. The private key is used to authorize operations from your wallet. This process is what is known as asymmetric cryptography.

New transactions are continually flowing through the network from all types of wallets and other applications and, when the nodes locate them, they are added to a temporary pool of unverified transactions. The miners will choose the operations of these Pools of unconfirmed Transactions to create a new block of transactions.

A block is a set of confirmed transactions. Each block is a part of the chain with the following elements:

- An alphanumeric code that links to the previous block.

- A package of transactions.

- Another alphanumeric code that will link to the back block.

A block must be added to the chain through a hash, that is, a part of the code generated from a series of mathematical operations.

**BLOCKCHAIN MINERY**

The miners are a crucial figure in the process that is dedicated to verifying the transactions that are occurring at the moment. The miners have two functions:

* Create new bitcoins for each block that is mined.
* Ensure that transactions are real and legitimate

They check that the time series is correct, that the proposed block is at the top of the main chain and that all operations within the block are valid.

The mining groups are groups of miners who work together to solve a block and divide the rewards granted to the miners. Currently, without a mining group, it is difficult to win an award. It is much more convenient to share the work and divide the bitcoins into a much larger group of miners.

**GENESIS BLOCK, MAIN BLOCK & ORPHAN BLOCK**

The Genesis block is the first block created in BlockChain. The successively worked bricks will be incorporated into the spine of the chain, called the Main Block.

When two miners are sent to the Pool of unconfirmed Transactions and manage to resolve the same block of transactions with a few seconds of difference, both emit their valid blocks to the network and, therefore, both can receive the corresponding reward.

However, some nodes will receive one block before the other (Block 1) and will begin to solve the next block (Block 1.1, Block 1.2, Block 1.3 ...) based on the hash of the block they received first. On the other hand, other nodes will receive a different block before (Block 2). And they will use its hash to solve the next block. It is at that moment when the rest of the nodes discard one of the blocks, the one with the fewest blocks ahead. These blocks are called orphan blocks.

**IS THE BLOCKCHAIN ​​THE NEXT TECHNOLOGICAL DISRUPTION?**

Now that you know how Blockchain works, you will be beginning to realize the infinite possibilities that it brings.

Bitcoin is a revolutionary breakthrough with the ability to transform the way audiences around the world interact and carry out operations. Sectors such as Financial, Legal, Energy, Health, Industry, Commerce, or Intellectual Property can be profoundly altered.

Many experts already see the Blockchain as the next significant technological disruption of the second decade of the 21st century.