Bitcoin Overview

Bitcoin works over a decentralized network, and it is important to know how bitcoin works and why its secure. It's important to know how bitcoin achieves decentralization knowing who : (i) maintains the ledger of transactions?, (ii) has authority over which transactions are valid?, (iii) creates new bitcoins?, (iv) determines how the rules of the system change?, and (v) how bitcoins acquire exchange value?

A key term related to bitcoin is consensus, that is used to know exactly which transactions were broadcast into the network and the order of these transactions. There are two big problems to obtain consensus on Bitcoin protocol: (i) network problems like latency or node crashing, and (ii) nodes trying to sabotage the process. Although these problems, there are some protocols that can be used to achieve consensus like Paxos protocol. Other problems that bitcoin needs to face up are, for example, nodes stealing bitcoins, denial of service attacks or double-spend attacks.

Another key point in bitcoin are the incentives that can be achieve in different ways like: (i) block reward, (ii) transaction fees, or (iii) mining and proof-of-work done (that will be realize using techniques like hash puzzles). Mining bitcoins is not an easy way to obtain bitcoins, due to is quite expensive (it needs an investment on equipment, electricity…) and bitcoin value is very volatile.

Basically, in a bitcoin transaction there are three parts: (i) a metadata that includes the needed information about the transaction like the size of the transaction, the number of inputs and outputs, (ii) transaction inputs, and (iii) transaction outputs (that contains scripts). These scripts can be used to escrow transactions (introducing a third party at the transaction), paying to a node that is offline at the moment of the transaction (using green addresses), efficient micro-payments, smart contracts…

To understand bitcoins, we need to understand the structure of a bitcoin chain, that is formed by: (i) a hash chain of blocks that links the different blocks, and (ii) an internal hash structure formed by a tree of all of the transactions that are included in that block.

Finally, it's important to point that there are some limitations of bitcoin like the limited total number of bitcoins in existence and as a consequence a needed change of rewards that due to the structure of the mining rewards it would have enormous economic consequences.