Hash functions allow bitcoin to grow and be secured. Bitcoin uses SHA-256 hash function which was the most secure when bitcoin was developed. In simple words hash functions are one-way encryption functions that links blocks. Each block contains hash in (any length) and out (fixed length). In other words, each input is given fingerprint by hash function, any change in input result in different output. Therefore, we can identify state of block just looking at one hash. Merkle trees are a data structure that can take “n” number of hashes and represent it with a single hash. In other words, we can look at the top hash in the block and verify the data. The role of Markle tree in Bitcoin is to store and prune data. It allows lightweight verification of bitcoin payments through checking longest blockchain headers, no need to download whole blockchain.

Bitcoin miners are backbone of Bitcoin. They validate transactions, stores blocks and decide which block to append. In non-technical words, miners are organizers of bitcoin. They collect all new transactions, make one block, and try to be the first one to add new block to the chain. If their block accepted, they get reward amount of 6.25 (1 February 2022) and transaction fee included of transactions in the block. The time and difficulty for finding new block is adjusted every 2 weeks (2016 blocks) and intended time to find each block is 10 minutes. As more miners are online difficulty increases, if decreases wise versa. Miners first used CPU, then GPU and now ASIC is most popular for cryptocurrency mining. Today, mining is not a hobby anymore, there are mining pools that collect big computing power and increase their chance of creating new valid block. However, there are concerns about energy usage, ecology and power dominance.