Bitcoin – Summary

Data structure

Bitcoin uses blocks which are a collection of transactions together with block headers. All the transactions are initially hashed, and then they are later organized into Merkle trees, which is structured like a binary tree in case of bitcoin. That way, the entire history of transactions/blockchain can be presented by a final root hash. The root hash can be used to ensure that there have been no modifications, this allows for less storage and computational requirements, which is an advantage of using Merkle trees and hashes.

Bitcoin mining

Bitcoin mining is necessary part of the process as there are people that need to verify all the transactions and blocks. There also needs to be an incentive to do this, which is why there is an award (in bitcoins) to miners that successfully find a block. What they need to do, is find a nonce that will produce a required hash for a specific block. This is very computationally expensive, and the uncertainty of success is what discourages small miners to operate. Most of the mining nowadays is done by mining pools, where many small miners join in a search for finding a nonce and share the award between themselves. This way, a much more predictable income is given for the miners. Bitcoin mining is not a very eco-friendly proccess, with the main concern being a huge amount of electricity that is being “wasted”.