A Review of Bitcoin Data Structures and Bitcoin Mining

Bitcoin has gotten a lot of media attention the past couple of years, with many people viewing it as a sort of “Get rich quick-scheme”. However, not a lot of people know what bitcoin really is, and how bitcoin mining works. The curriculum this week aims to shed light upon this, namely what bitcoin is, and how mining works. At first, we are presented with what Merkle trees are, how they work and their purpose in Bitcoin. The business case of mining is also explained. Then, it is explained how Bitcoin is mined. Alternative ways of mining are also suggested.

To summarize, a Merkle tree is a hash based data structure. As for bitcoin, the leaf nodes are transactions. The nodes that are not leafs, are the hash of its children. Thus, a change in one of the transactions will force a change in the entire tree.

There are plenty of similarities between the history of bitcoin mining and the history of gold mining. Both started with amateurs competing against each other with the goal of quick money. Both have now ended up professionalized and unviable for small scale actors.

To start mining bitcoin you first need to listen to the transactions in the network and validate them. You need to maintain the blockchain and listen for new blocks. Then you need to put together a candidate block. This is the block that you are going to propose. Finally you need to solve an energy intensive cryptographic puzzle. This is called proof of work. If you are able to solve the puzzle, you can broadcast the block to the rest of the network and hope it gets accepted. If it does, you can pop the champagne.

The proof of work scheme has faced a lot of criticism in recent times, due to its energy consumption. Therefore alternative schemes such as proof of stake have been proposed.

There is no new perspective on the topic, neither are there any new theories. It is however a useful description of how bitcoin mining works both technically and business-wise.

The book gives the not too technically gifted reader an understandable introduction to bitcoin mining. (Tschorsch & Scheuermann) offers a more comprehensive discussion on the topic of Proof of X which may satisfy the more tech savvy reader. I find the research interesting. Especially what is said about more energy efficient Proof of X-schemes. I also enjoyed reading about the parallel between gold mining and bitcoin mining.