Mining in Bitcoin

IN5420 Distributed Blockchain Technologies

Michael Eikeland

February 2018

1 Bitcoin mining

While mining is something that at first glance seems to be a purely financial motivated aspect of Bitcoin, the purpose of it is somewhat more complex. By encforcing the rulesets of the Bitcoin protocol, miners are the reason the decentralized Bitcoin network is able to achieve distributed consensus. By producing valid blocks - essentially confirming pending transactions - miners move the Bitcoin block chain forward at a predictable and decidable interval.

When a miner is up-to-date on the blockchain and listening for incoming transactions it may start producing candidate blocks in hopes of eventually finding a valid block. Once a valid block is found the miner announces it to the network and hopes that the network will use this block as a base for the next block. The miner that finds the block is entitled to a block reward - currently 12.5 Bitcoins which at the time of writing has a market value of 950,000 USD - along with any transaction fees - the remainder of all transactions in the block that have no output assigned. This is the incentive that drive people to participate in mining as mining can be quite costly in terms of equipment and energy consumption.

Some other remarks:

- **Mining hardware:** Typical computer parts such as the CPU and GPU are designed for multiple purposes and use cases. For specialized actions, such as mining, specialized hardware will achieve much better performance than all-purpose hardware. This is profitable for miners, and as such they have invested in ASIC (Application-specific integrated circuit) mining equipment. In turn this has increased the hash rate of the Bitcoin network and consequentially increased the difficulty target in the Bitcoin network.

- **Energy consumption:** Miners use a lot of energy, and one can argue that since mining is purposely designed to require a lot of guess work it is a waste of energy. The topic has been quite controversial and reports show that the Bitcoin network is estimated to use more electricity than several developed countries[Bitcoin Energy Consumption].

- **Mining pools:** As the difficulty of finding new blocks individually has increased, miners have started to organizing themselves in *mining pools* where the nonce search space is split between the miners in order to find blocks faster. The block claim reward is usually split between the miners based on how much computation they are estimated to have performed.

2 Alternative mining

If one were to change or improve on Bitcoin's puzzle a desired trait would be that every miner has a chance of finding a new block proportional to their work performed. Another discussed trait is that puzzles should be ASIC-resistant in order to level the playing field between professional miners and regular users. There is a discussion to make the proof-of-work method ”useful”, similar to earlier scientific efforts such as Folding@Home. For reasons similar to make puzzles ASIC-resistant, there is also a desire to avoid the formation of mining pools as these potentially become big enough to hold the majority of the hashing power and in turn threaten the integrity of Bitcoin.