COMP3632 - Homework 4

Samuel Petit
20683298

Question 1

a) There are 10^20/10^16 = 10^4 miners in total. The cost for running the rig for 10 minutes is of 0.002 * 60*10 = 1.2$. So we expect each miner to get 6/10^4 = 6 * 10^-4 BTC. Thus we have the following equation : 6*10^-4 * x = 1.2 ⇔ x = 2000$. We need a bitcoin to be worth **at least 2000$** in order for the miners to not lose money.
b) We have blocks of 1MB and a transaction is at least 166MB thus the maximum amount of transactions per block is 1048576/166 = 6316.72 → there are a maximum of 6316 transactions per 10 mins, that is 6316/(60*10) = 10.52 → **10 transactions per second at most**.
c) Miners now need to make half of their income by transaction since it was cut in half. That is about 0.5 * 0.002 * 60*10 = 0.6$. Thus we get the following equation : 0.6 = fee * number of transactions / number of miners. Since we have 10^20/10^16 = 10^4 miners and 1048576/166 = 6316 transactions we get 0.6 = fee * 6316/10^4 ⇔ **fee = 0.9599$.**

Question 2

a) Proof of stake does not require miners to brute force hashes. It still acts such that transactions are verified without a third party. Here individuals creates the next block based on their stake (how much of the crypto currency they own). Instead of mining they are betting on the blocks that will be added to the chain with a reward in proportion to their stake if they are right. This also makes for a more fair reward system (linear) when comparing with the Proof of work system where it is attributed to the miner to find the hash.
b) There are different points of comparison. The first one is that the Proof of Work system consumes a lot more electricity than PoS does. There is also the fact that PoW does not scale well and PoS scales a lot better in comparison. In PoS a 51% attack is also much less likely since you would risk losing your stake in that crypto currency, on the other hand PoW doesn't have much of a protection against a 51% attack. The reward system of PoS is also more fair (and linear) than that of PoW which has more of an exponential curve in terms of investment/reward potential.

Question 3

a) The risk with using block.timestamp is that it can be manipulated by the attacker. This is particularly dangerous with a gambling game or when mining cryptocurrencies block.timestamp, is the value what miner decides to publish there when s/he finds a block, since it can be manipulated by a miner, we should not trust a miner for picking the time.
b) RANDAO is a system in which everyone contributes to picking a time. Each of the miners publish a value that they have hashed. We combine all of the numbers and obtain a safer value than we would if we let a single miner pick the time. It however

also has weaknesses because of the values being combined together. An attacker could theoretically calculate the final value and reveal a different value.

Question 4

a) Data poisoning is when an attacker is able to inject or manipulate the training data of a model. Attacks may target availability: this would make the capabilities of the model to be incorrect. Another type of attack may be the integrity attack (the backdoor attack) : here the attacker can essentially get the model to do what it wants by giving it an input unknown to the designer.
b) Data sanitisation is used to identify and remove errors, duplicates, invalid and unwanted data from a dataset. It is used to create a reliable and useful dataset and generally improve its quality. It can be done in multiple ways such as using scripts, with data wrangling tools or as batch processing...