TTM4195 - Blockchain Technologies and Cryptocurrencies
Assignment 1

Jonathan Brooks

21.09.2020

1 Introduction

From the specifications we were supposed to find a Bitcoin block from 2018, with the last three digits matching the last three digits of my student number (504896) and containing at least 10 transactions. After some filtering and sorting on BlockChair [1] I found the block 548896 [2] that matched those qualifications.
Target Block: 548896
Target day: 5th of November 2018

2 Questions

1. How many Bitcoins have been issued up to and including your target block? How many Bitcoins will eventually be issued after your target block? Explain how you calculate these values.

    - I used Coinmamas [3] numbers on when halving happened to calculate how many Bitcoins that have been issued. From block 0 to 210 000 the block reward was 50 BTC, therefore in this period 10 500 000 BTC were issued. After that the block reward was halved to 25 BTC until block 420 000, in this period 5 250 000 BTC were issued. And after block 420 000 the reward was halved again to 12.5 BTC, so when using my chosen block as the end point we can calculate that there were issued 1 611 200 BTC in this period. So all in all, there were issued 17 361 200 BTC up to and including my block.
    - Since the maximum number of Bitcoins to ever exist is hard coded to be 21 000 000, we can very easily calculate how many Bitcoins that will be issued after my block by just taking 21 000 000 - 17 361 200 which is 3 638 800 Bitcoins.

2. What was the maximum and minimum transaction fee paid on your target day? What was the largest and smallest number of transactions in a block on your target day? For each answer, discuss briefly why the values might vary

    - The largest transaction fee paid on my target day was 0.01253071 BTC [4] and the smallest was 0 BTC [5]. The 0 BTC fee was due to the transaction being a "Create new Bitcoin" transaction. The large gap could be a result of there being a lot of people who wanted to get their transaction onto the blockchain at the same time, and therefore being willing to pay a higher fee so that the miners would include them on their block.
    - The largest number of transactions on a block on my target day was 3429 transactions [6], while the smallest amount of transactions on a block was 1 [7]. This variation is just the result of there being more people that were using Bitcoin when the block with the higher transaction number was being constructed, than there were with the lower transaction number block.

3. When was the last change in difficulty before your target day? What was the latest (newest) block before your target block where difficulty decreased compared to the previous one? Why is this unusual and why might it have happened?

    - The last change of difficulty before my target day was after block 548351, where it went from 7,182,852,313,938.30 to 7,184,404,942,701.80. The reason for the increase was probably that the total mining hash rate increased, so they increased the difficulty to keep up with the 10 minute per block rule.
    - From block 546335 to 546336 the difficulty decreased with about 2116334325. This is unusual since Bitcoin is usually a little bit profitable to mine, but when there are too many miners and the smaller miners can't keep up with the bigger miners they have to give up and turn of their mining machines. When they turn off their machines the total mining hash rate will go down, which in turn will decrease the difficulty.

4. Find the time for each block on your target day. Call the time between two successive blocks the inter-block time.

   (a) How many instances of an inter-block time greater than 20 minutes occurred on your target day?

   (b) How many instances of an inter-block time greater than 30 minutes occurred on your target day?

   Discuss whether your findings match the assumption that inter-block time is governed by an exponential distribution with average rate 10 minutes.

   - From the script I made I found that 22 inter-block times on my target day was over 20 minutes, and that 6 inter-block times were over 30 minutes. I found the timestamps using the btc.com [8] API, were the timestamps are posted in seconds.
   - The number of blocks on my target day was 144. By using the formula:

     $$Pr(X \leq x) = 1 - e^{-x/10} \tag{1}$$

     provided in lecture 4, we can find the probability of a block appearing in x minutes. So we can calculate the probability of a block appearing in 20 and 30 minutes by doing:

     $$Pr(X \leq 20) = 1 - e^{-2} = 0.86 \tag{2}$$

     $$Pr(X \leq 30) = 1 - e^{-3} = 0.95 \tag{3}$$

     This means that there is a 14% chance for a block to take more than 20 minutes to appear, and there is a 5% chance for a block to take more than 30 minutes. 14% of 144 is about 20 and 5% of 144 is about 7. Which means that my findings match the assumption that inter-block time is governed by an exponential distribution pretty well.

5. How many different (non-overlapping) 10-minute intervals with at least 3 blocks in that interval occurred on your target day? Discuss whether your findings match the assumption that the number of blocks in an interval is governed by a Poisson distribution.

   - From my calculations by using the same API as before [8], I found that 7 10-minute intervals contained 3 or more blocks. By using the Poisson distribution formula:

     $$Pr(X = k) = 1/(e * k!) \tag{4}$$

     So if we calculate with k = 3:

     $$Pr(X = 3) = 1/(e * 3!) = 1/(e * 6) = 0,0613 \tag{5}$$

     we find that 6% of the intervals should contain 3 blocks or more. We can then calculate that 6% of 144 is 8,6, which is very close to what I got when using the practical tests.

References

[1] https://blockchair.com/

[2] https://blockchair.com/bitcoin/block/548896

[3] https://www.coinmama.com/blog/the-bitcoin-halving-a-history/

[4] https://blockchair.com/bitcoin/transaction/354173824

[5] https://blockchair.com/bitcoin/transaction/354045146

[6] https://blockchair.com/bitcoin/block/548935

[7] https://blockchair.com/bitcoin/block/548797

[8] https://btc.com/api-doc