Report HW2

Kumaran Kartikeyan (23M0803)
Sarthak Sharma (23M0789)
Pulkit Suhag (23M0782)

Conclusion:

Changes due to change in n:

If we increase the value of n then the number of forks would increase and thus the orphan blocks would also increase, but it has less effect on the implementation on the double spend attack. As even though the nodes are high there overall hashing power remains the same.

Changes due to change in Ttx (transaction time):

If we increase the transaction generation time then the transactions will reach all nodes and if the selfish miner tries to implement the same transactions then the blocks verification would also be easier for other blocks. But increasing the Ttx then the efficiency would decrease.

Changes due to change in Tk (Mean block generation time):

Decreasing Tk too much may lead to increased orphaned blocks and chain reorganizations, as multiple miners may find valid blocks simultaneously, causing temporary forks in the blockchain.

Changes in the values of ζ1 and ζ2 (The individual hashing power of selfish miner 1 and 2):

There are further 4 possible scenarios from our observations:

High Difference in Hashing Power:

If one selfish node has higher hashing power than another. Then most of the blocks would be his own. The dominant selfish node will have a higher probability of mining blocks faster than both the honest nodes and the weaker selfish node. The attack would be predictable with the most number of orphan blocks generated by the dominant one. The dominant selfish node would release longer chains releasing a long chain, in which even higher number of confirmation would also fail

Low Difference in Hashing Power:

If the two selfish nodes have similar levels of hashing power, Then if both the selfish miners have less hashing power than as there is no coordination between the miners then therefore it would be hard to implement the double spend attack and most of the blocks would be honest. If it is higher then there would almost be high chances of double spend attack from both the selfish miners, and even higher amount of orphan blocks. There would be high competition between the selfish nodes and also the honest ones.

Low Hashing Power Overall:

If the overall values of hashing power for both selfish nodes are low, The selfish nodes may struggle to maintain longer secret chains compared to scenarios with higher hashing power. Therefore the scenario would be close to the normal working of blockchain.

High Hashing Power Overall:

With high hashing power for both selfish nodes. The selfish nodes will have a greater ability to overpower the honest nodes and execute successful double spend attacks. There would be high number of forks, orphan blocks and attacks.