CS 765 : Report - Project Part 2

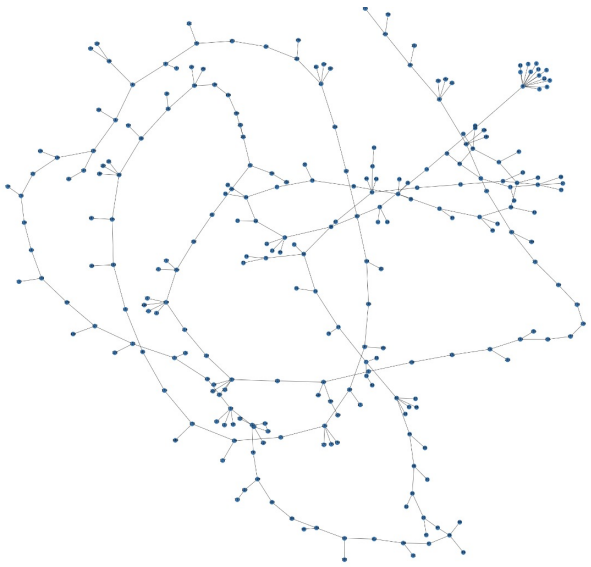
Simulating a selfish mining attack using the P2P Cryptocurrency

Aakriti - 190050002
Aditya Badola - 190050006
Gaurang Dev - 19D070024

October 17, 2021

1 Terminology and Assumptions

- Simulation time is taken to be $500s$.
- We have taken number of peers (N) to be 20 instead of 100. This is because, the visualisations are better for smaller N. For large enough Ns, the blockchain trees were cluttered and inconclusive.
  We experimented for $N = 100$, simulation time $= 100s$ and obtained the following blockchain tree for the default parameters:



- For each experiment, we have included the following in the report:

MPU Adversary	$\frac{\text{\# blocks mined by adversary in main chain}}{\text{total \# blocks mined by adversary}}$
MPU Overall	$\frac{\text{\# blocks in main chain}}{\text{total \# blocks mined by all nodes}}$
Effective α	$\frac{\text{\# blocks mined by adversary in main chain}}{\text{total \# blocks in the main chain}}$

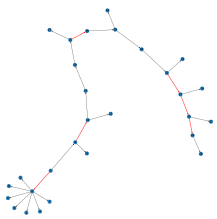
- There is also an 'Upper bound on effective α'. This is because, at the end of simulation, the adversary might have had a lead but could not release her private chain. So, this bound takes into account the situation when the adversary was able to release her private chain.
- Note that the simulations may not show a trend, because the experiments are non-deterministic. There is randomness involved in terms of latency, inter-arrival time between blocks and transactions, etc.
- **In the blockchain plots that follow, the red lines indicate that the block that follows it, is created by the adversary.**

2 Selfish Miner

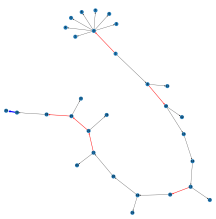
2.1 Variation with fraction of nodes, an adversary is connected to (ζ)

Keeping $N = 20$, $\lambda_{tx} = 0.5$, $\lambda_k = 0.0025$, $\alpha = 0.3$ constant.
As ζ increases, more fraction of honest nodes are connected to the adversary. So, the adversary will be able to broadcast her blocks to a greater extent when at state $lead = 0'$. That is, γ increases, increasing the effective α and MPU Adversary.
Following are the blockchains for an honest peer and the adversary:

- **Case 1:** $\zeta = 0.25$



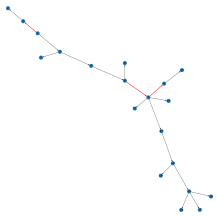
(a) An honest peer



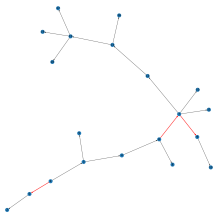
(b) Selfish miner

MPU Adversary	0.714286
MPU Overall	0.5
Effective α	0.333333
Upper bound on effective α	0.375

- **Case 2:** $\zeta = 0.5$



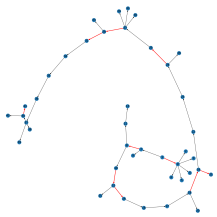
(a) An honest peer



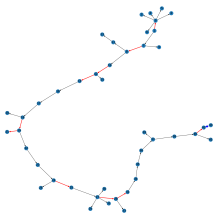
(b) Selfish miner

MPU Adversary	1
MPU Overall	0.55
Effective α	0.272727
Upper bound on effective α	0.272727

- **Case 3:** $\zeta = 0.75$



(a) An honest peer



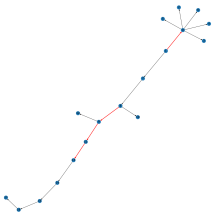
(b) Selfish miner

MPU Adversary	0.818182
MPU Overall	0.568182
Effective α	0.36
Upper bound on effective α	0.384615

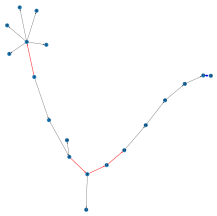
2.2 Variation with mean inter-arrival time between blocks (λ_k)

Keeping $N = 20$, $\lambda_{tx} = 0.5$, $\zeta = 0.5$, $\alpha = 0.3$ constant.
As $T_k(\propto \frac{1}{\lambda_k})$ increases, the inter-arrival time between two consecutive blocks increases. So, less number of blocks will be generated given the simulation time, and therefore, there will be lesser branching. Due to less branching, lesser blocks are discarded because of forking. So, MPU overall increases. There is no conclusive effect on MPU Adversary and effective α.
Following are the blockchains for an honest peer and the adversary:

- **Case 1:** $\lambda_k = 0.001$



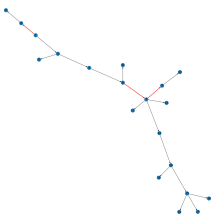
(a) An honest peer



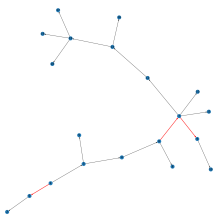
(b) Selfish miner

MPU Adversary	1
MPU Overall	0.578947
Effective α	0.363636
Upper bound on effective α	0.416667

- **Case 2:** $\lambda_k = 0.0025$



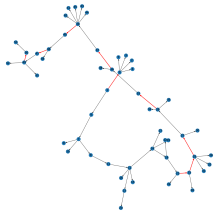
(a) An honest peer



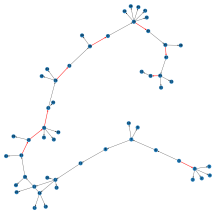
(b) Selfish miner

MPU Adversary	0.714286
MPU Overall	0.5
Effective α	0.333333
Upper bound on effective α	0.375

- **Case 3:** $\lambda_k = 0.005$



(a) An honest peer



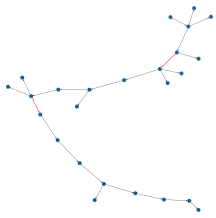
(b) Selfish miner

MPU Adversary	1
MPU Overall	0.444444
Effective α	0.375
Upper bound on effective α	0.375

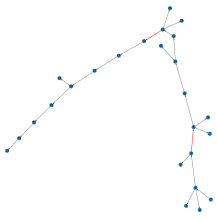
2.3 Variation with hashing power of adversary (α)

Keeping $N = 20$, $\lambda_{tx} = 0.5$, $\lambda_k = 0.0025$, $\zeta = 0.5$ constant.
As α increases, the hashing power of the adversary increases. So, the selfish miner will mine blocks more often, giving the advantage to grow her private chain longer, therefore discarding the efforts of honest miners. So, effective α will increase more rapidly as α increases. MPU Adversary increases. MPU Overall steadily decreases. Forking increases since the adversary has more resources and mines blocks more often.
Following are the blockchains for an honest peer and the adversary:

- **Case 1:** $\alpha = 0.1$



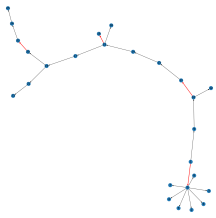
(a) An honest peer



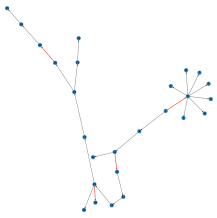
(b) Selfish miner

MPU Adversary	1
MPU Overall	0.6
Effective α	0.133333
Upper bound on effective α	0.133333

- **Case 2:** $\alpha = 0.2$



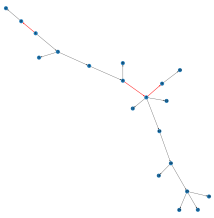
(a) An honest peer



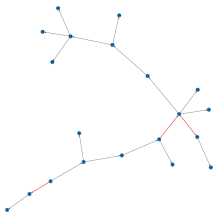
(b) Selfish miner

MPU Adversary	1
MPU Overall	0.515152
Effective α	0.294118
Upper bound on effective α	0.294118

- **Case 3:** $\alpha = 0.3$



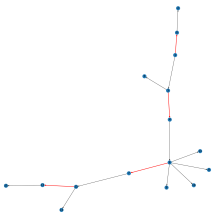
(a) An honest peer



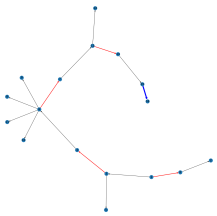
(b) Selfish miner

MPU Adversary	1
MPU Overall	0.55
Effective α	0.272727
Upper bound on effective α	0.272727

- **Case 4:** $\alpha = 0.4$



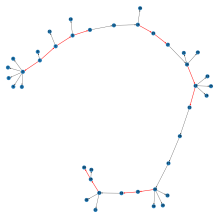
(a) An honest peer



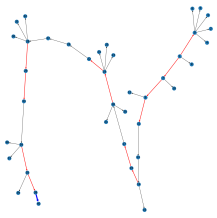
(b) Selfish miner

MPU Adversary	0.8
MPU Overall	0.529412
Effective α	0.444444
Upper bound on effective α	0.5

- **Case 5:** $\alpha = 0.5$



(a) An honest peer



(b) Selfish miner

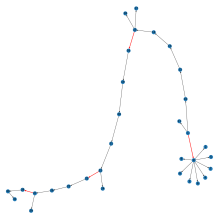
MPU Adversary	1
MPU Overall	0.487805
Effective α	0.6
Upper bound on effective α	0.619048

3 Stubborn Miner

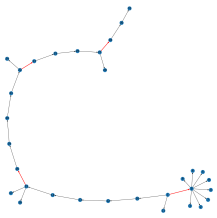
3.1 Variation with fraction of nodes, an adversary is connected to (ζ)

Keeping $N = 20$, $\lambda_{tx} = 0.5$, $\lambda_k = 0.0025$, $\alpha = 0.3$ constant.
As ζ increases, more fraction of honest nodes are connected to the adversary. So, the adversary will be able to broadcast her blocks to a greater extent when at state $lead = 0'$. That is, γ increases, increasing the effective α and MPU Adversary.
Following are the blockchains for an honest peer and the adversary:

- **Case 1:** $\zeta = 0.25$



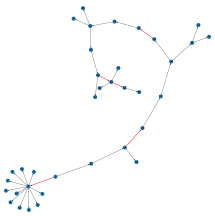
(a) An honest peer



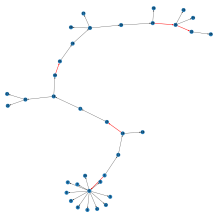
(b) Stubborn miner

MPU Adversary	1
MPU Overall	0.59375
Effective α	0.210526
Upper bound on effective α	0.210526

- **Case 2:** $\zeta = 0.5$



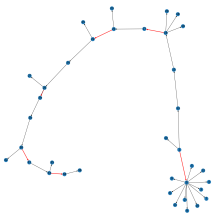
(a) An honest peer



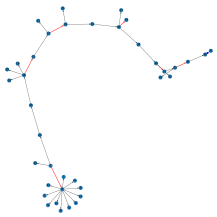
(b) Stubborn miner

MPU Adversary	1
MPU Overall	0.444444
Effective α	0.3125
Upper bound on effective α	0.3125

- **Case 3:** $\zeta = 0.75$



(a) An honest peer



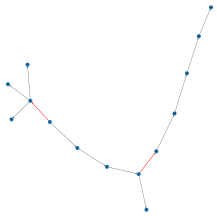
(b) Stubborn miner

MPU Adversary	0.714286
MPU Overall	0.421053
Effective α	0.3125
Upper bound on effective α	0.352941

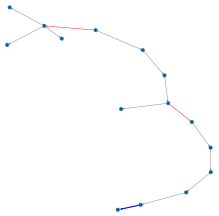
3.2 Variation with mean inter-arrival time between blocks (λ_k)

Keeping $N = 20$, $\lambda_{tx} = 0.5$, $\zeta = 0.5$, $\alpha = 0.3$ constant.
As $T_k(\propto \frac{1}{\lambda_k})$ increases, the inter-arrival time between two consecutive blocks increases. So, less number of blocks will be generated given the simulation time, and therefore, there will be lesser branching. Due to less branching, lesser blocks are discarded because of forking. So, MPU overall increases. There is no conclusive effect on MPU Adversary and effective α.
Following are the blockchains for an honest peer and the adversary:

- **Case 1:** $\lambda_k = 0.001$



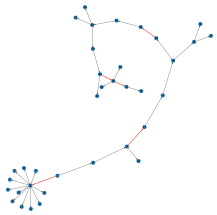
(a) An honest peer



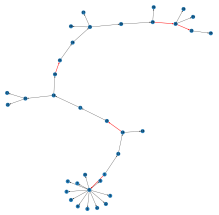
(b) Stubborn miner

MPU Adversary	0.666667
MPU Overall	0.666667
Effective α	0.2
Upper bound on effective α	0.272727

- **Case 2:** $\lambda_k = 0.0025$



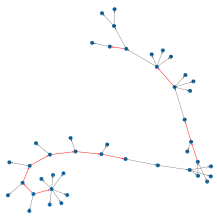
(a) An honest peer



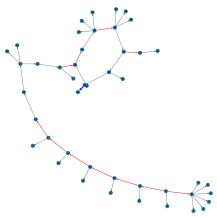
(b) Stubborn miner

MPU Adversary	1
MPU Overall	0.444444
Effective α	0.3125
Upper bound on effective α	0.3125

- **Case 3:** $\lambda_k = 0.005$



(a) An honest peer



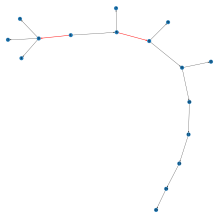
(b) Stubborn miner

MPU Adversary	0.833333
MPU Overall	0.422222
Effective α	0.526316
Upper bound on effective α	0.55

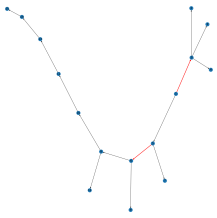
3.3 Variation with hashing power of adversary (α)

Keeping $N = 20$, $\lambda_{tx} = 0.5$, $\lambda_k = 0.0025$, $\zeta = 0.5$ constant.
As α increases, the hashing power of the adversary increases. So, the stubborn miner will mine blocks more often, giving the advantage to grow her private chain longer, therefore discarding the efforts of honest miners. So, effective α will increase more rapidly as α increases. MPU Adversary increases. MPU Overall steadily decreases. Forking increases since the adversary has more resources and mines blocks more often.
Following are the blockchains for an honest peer and the adversary:

- **Case 1:** $\alpha = 0.1$



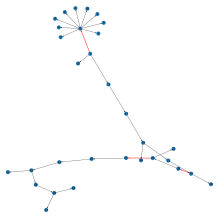
(a) An honest peer



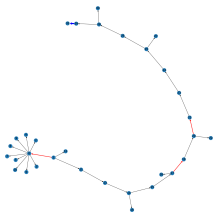
(b) Stubborn miner

MPU Adversary	1
MPU Overall	0.625
Effective α	0.2
Upper bound on effective α	0.2

- **Case 2:** $\alpha = 0.2$



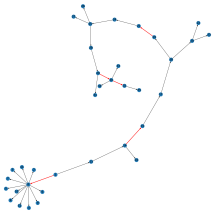
(a) An honest peer



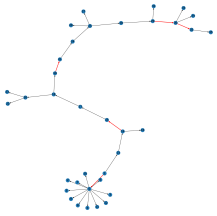
(b) Stubborn miner

MPU Adversary	0.5
MPU Overall	0.5
Effective α	0.125
Upper bound on effective α	0.176471

- **Case 3:** $\alpha = 0.3$



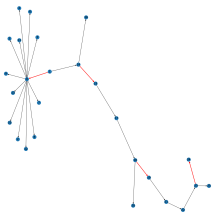
(a) An honest peer



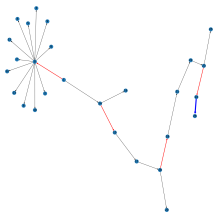
(b) Stubborn miner

MPU Adversary	1
MPU Overall	0.444444
Effective α	0.3125
Upper bound on effective α	0.3125

- **Case 4:** $\alpha = 0.4$



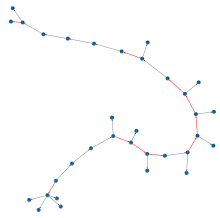
(a) An honest peer



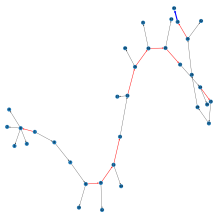
(b) Stubborn miner

MPU Adversary	0.8
MPU Overall	0.407407
Effective α	0.363636
Upper bound on effective α	0.416667

- **Case 5:** $\alpha = 0.5$



(a) An honest peer



(b) Stubborn miner

MPU Adversary	0.909091
MPU Overall	0.588235
Effective α	0.5
Upper bound on effective α	0.52381

4 Comparision between Selfish and Stubborn miners

It can be observed that selfish mining is not the optimal malicious type of mining. Stubborn mining is more profitable since it holds back blocks more often discarding the blocks generated by honest blocks frequently. Although the results are not very clear indicative of that, this is because these are just a few tens of experiments performed under restricted N and simulation time.

5 Theoretical $\gamma = 0$, $\gamma = 1$ along with selfish, stubborn plots

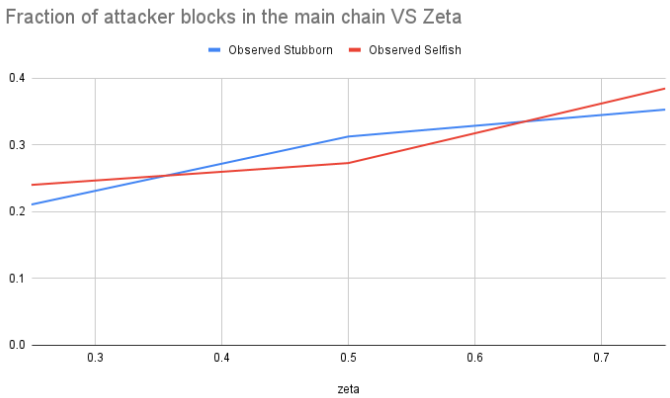


Figure 23: Variation with ζ

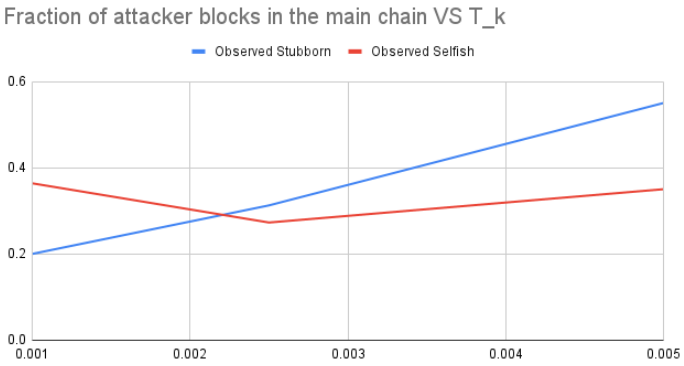


Figure 24: Variation with λ_k

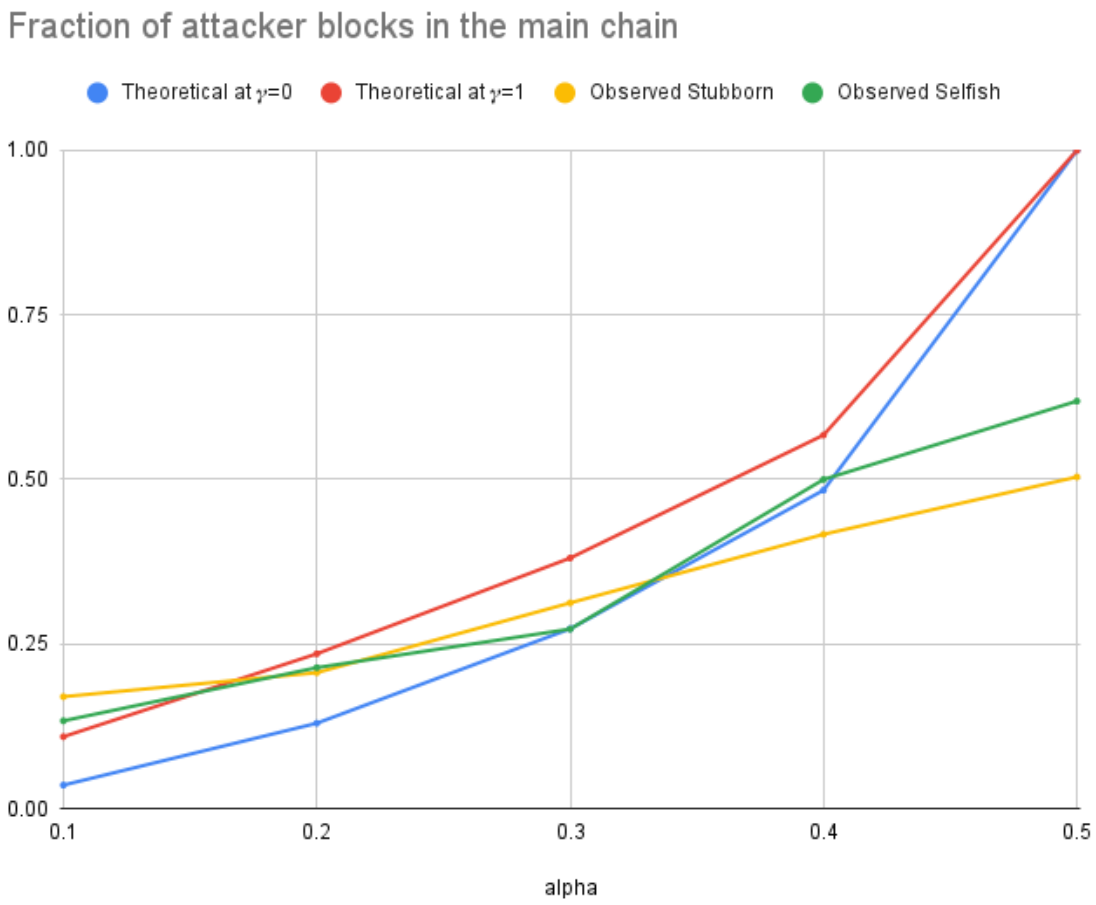


Figure 25: Variation with α