Blockchain Assignment 2

Yashvardhan, 200050162
Koustubh Rao, 200100176
Onkar Borade, 200050022
Neeshi Merchant, 200050087

March 2023

1 Description

- In the assignment statement, there are three kinds of hashing power: (i) Low (ii) High (iii) Adversarial hashing power
- ζ is the fraction of node connected to the attacker is a configurable parameter and will be set to $25\%, 50\%$and 75% in the demo.
- The malicious node is always fast.
- There are four categories of peers in addition to the attacker based on a peer's hash strength, which can be Low or High, and network speed, which can be Fast or Slow.
- The attacker does not forward any block generated by other nodes.

Definition 1.1. MPU_adv = (# Adversary blocks in main chain) / (# Total blocks mined by adversary).

Definition 1.2. MPU_overall = (# Blocks in main chain) / (# Total blocks across all peers)

Command Line Parameters

–n	number of peers in the network
–z0	fraction of slow peers
–z1	fraction of low cpu peers
–l	fraction of honest nodes adversary is connected to
–s	type of adversary choose from (0-selfish, 1-stubborn)
–p	fraction of hash power of attacker

2 Comparisons of Two Attack

2.1 Selfish Mining

The goal of the Selfish Mining Attack is for the selfish miner (Adversary) to fork the chain on purpose by keeping her found blocks private. The enemy mines on its own secret branch, while the honest nodes continue to mine on the public chain.

The enemy gains a bigger advantage over the public chain and keeps these new blocks private if she mines additional blocks. She makes blocks from the opponent's private chain visible to the public once the length of the public branch reaches that of the private branch of the adversary.

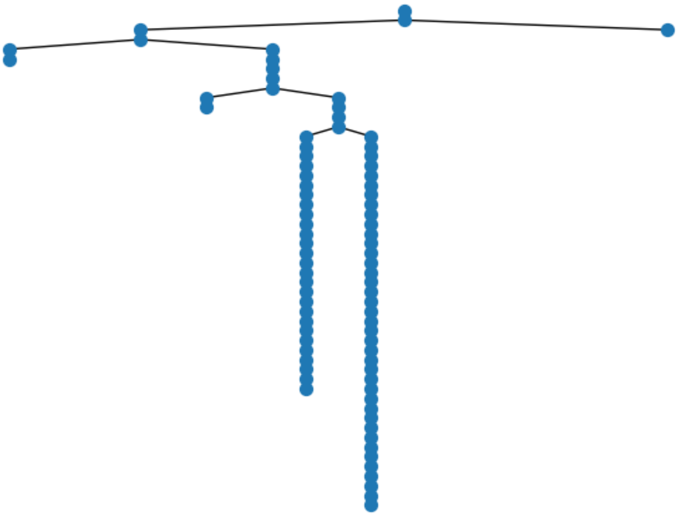

Figure 1: Selfish

2.2 Stubborn Mining

Stubborn Mining Attack aims to keep competition with the honest chain going. In order to maintain the forks for the longest chain rather than fully eliminating the honest chain, the adversary only reveals the next block on her private chain to match the length of the public chain rather than revealing the whole private chain.

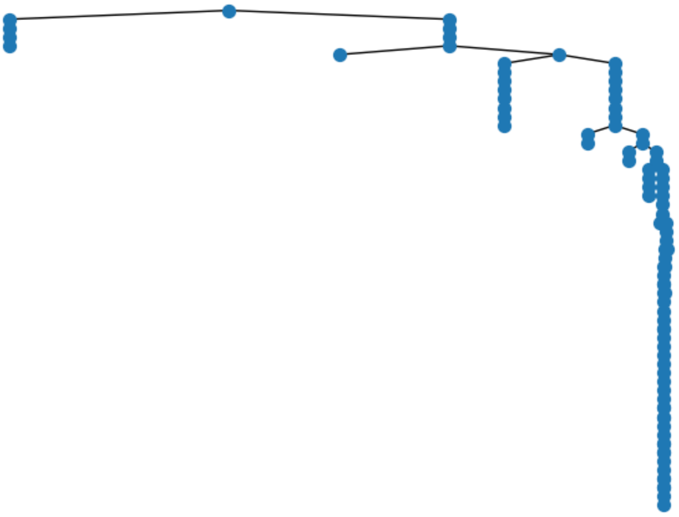

Figure 2: Stubborn

2.3 Result

2.3.1 Selfish Mining

As seen in the blockchain tree, a selfish miner kills the honest chain whenever it catches up to the private chain, resulting in a minor fork, although the majority of forks in selfish mining attacks are made up of a single block.

2.3.2 Stubborn Mining

As seen in the blockchain trees above, in the case of a stubborn miner's attack, the majority of forks are made up of many blocks since, as was said above, the adversary permits the honest chain to expand as well.

2.4 Remaks

In our analysis, we observed that selfish mining attacks are favored for low mining power values whereas stubborn mining is more advantageous for adversaries with mining powers near 0.5. This may be because the chain is never killed by the stubborn, and in the event that the chain has less hashing power, it may waste its mining efforts if the honest chain prevails. The effort of sincere miners is successfully wasted by obstinate miners with great hashing power, providing a better return than selfish mining assaults.

3 Analysis

Selfish Mining Attack

Alpha	0.1	0.2	0.3	0.4	0.5
ζ	0.5				
MPU_avd	0.67537	0.69953	0.81169	0.87902	0.97830
MPU_overall	0.92367	0.85145	0.86114	0.72896	0.57640
gamma_0	0.03664	0.13066	0.26813	0.48433	1.00000
gamma_1	0.11018	0.25322	0.37963	0.57244	1.00000
R_pool	0.09121	0.22219	0.24809	0.50704	0.84783

Stubborn Mining Attack

Alpha	0.1	0.2	0.3	0.4	0.5
ζ	0.5				
MPU_avd	0.33333	0.08726	0.23327	0.45423	1.00000
MPU_overall	0.82705	0.78083	0.77083	0.56289	0.51143
R_pool	0.06213	0.02667	0.06677	0.36235	0.97455

The MPU_adv and MPU_overall trend are opposing trends in the selfish mining attack, as we see. The general trend is that as the adversary's hashing power α increases the MPU_adv also increases as expected more proportions of its block should end up in the longest chain. The MPU_overall will consequently drop as a result of fewer honest blocks being added to the main chain as more blocks produced by honest miners are killed and honest miners' efforts and power are wasted.
Since there is a higher chance for stubborn blocks to be rejected by the network because they don't directly harm the honest chain, the ratio for the stubborn mining attack initially drops as hashing power rises. So, as hashing power rises, the adversary mines more blocks, but the majority of them are rejected (as seen by the R pool ratio), resulting in a lower percentage of blocks in the main chain. After alpha=0.2, the adversary benefits from the mining power, and we see that MPU_adv rises with alpha. The trend for MPU overall resembles the selfish mining attack. As the share of honest miners' hashing power falls, the ratio as a whole goes down. Hence, the enemy can obtain more trustworthy blocks to waste.

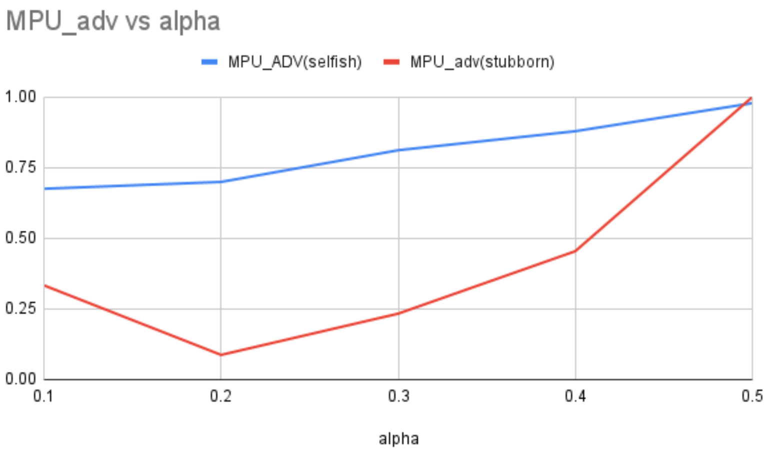

Figure 3: MPU_adv vs Alpha

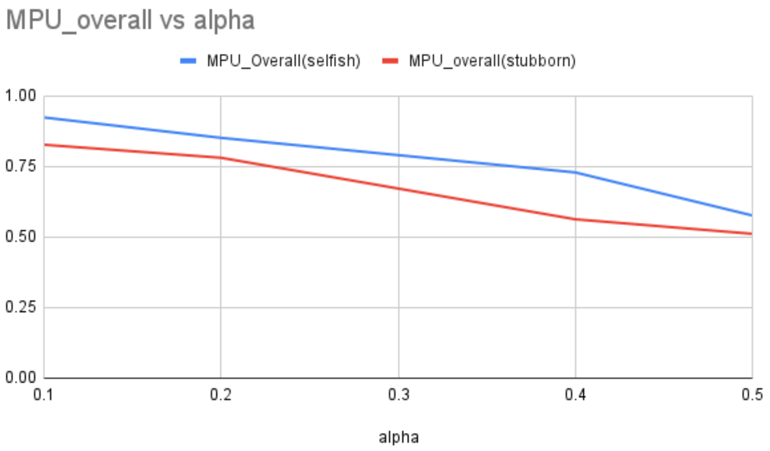

Figure 4: MPU_overall vs Alpha

3.1 Variation with Zeta

3.1.1 Selfish Mining Attack

The table and plots show that the MPU adv value in the selfish mining attack has a small peak at zeta 0.5. This is because as the adversary's connections with trustworthy peers grow, it continues to receive updates on newly produced blocks more quickly. The adversary can begin mining on the new honest block anytime it loses the race to make a block earlier. When zeta is low, the adversary will take longer to obtain the block and will continue mining on the previously existing block even if an honest block is created.
As a result, for smaller zeta values, the attacker will make fewer switches to the honest blockchain, resulting in a lower total number of blocks (the MPU adv denominator) and higher MPU adv values. An attacker benefits from growing zeta because honest peers will start mining on the attacker's blocks more frequently and will therefore obtain their blocks sooner. This helps the attacker get a larger percentage of its blocks into the blockchain. As a result, the effects of low and high zeta values are compromised. The ideal zeta should therefore be attained somewhere in the center, as is precisely seen in the maximum at zeta 0.5.

Selfish Mining Attack

ζ	0.25	0.50	0.75	1
α	0.35			
MPU_avd	0.79231	0.94355	0.86111	0.86111
MPU_overall	0.82958	0.79798	0.81512	0.79787
R_pool	0.28443	0.41772	0.39241	0.41333
gamma_0	0.36651			
gamma_1	0.46556			

3.1.2 Stubborn mining

The MPU adv graph shows that the parameter zeta is crucial in case of a stubborn mining attempt. This is because stubborn mining heavily depends on winning every block. Because more honest blocks will mine on the adversary's block as soon as they receive it, the likelihood that the adversary's block will prevail in the competition increases with the number of the adversary's direct links.

Stubborn Mining Attack

ζ	0.25	0.50	0.75	1
α	0.35			
MPU_avd	0.00000	0.12600	0.47987	0.83333
MPU_overall	0.69072	0.64211	0.68041	0.62626
R_pool	0.00000	0.06557	0.22727	0.48387

3.1.3 Concluding remarks

The MPU_overall in both attacks remains more or less constant and is not affected much by varying the zeta parameter. Although we see a slight decrease in the MPU_overall ratio which is expected since MPU_adv is increasing and as MPU_adv increases, honest miners' blocks will struggle to get into the chain, thus decreasing the MPU_overall ratio.

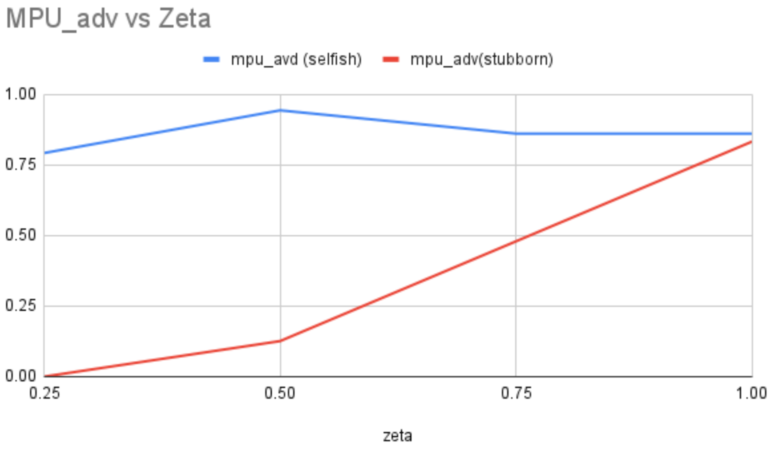

Figure 5: MPU_adv vs Zeta

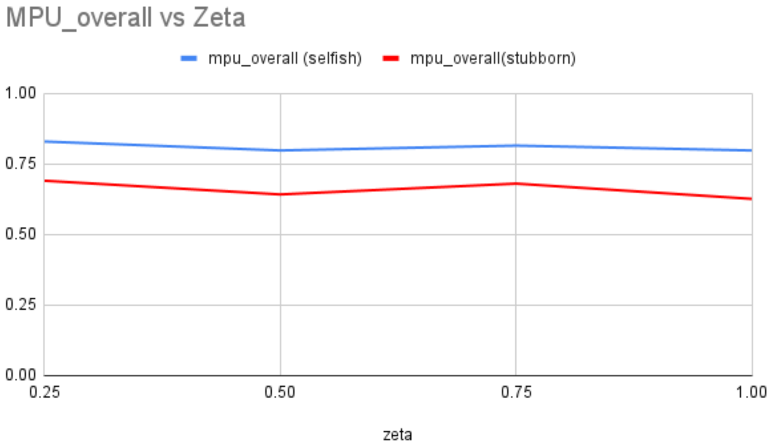

Figure 6: MPU_adv vs Zeta