Simulation of attacks on P2P Cryptocurrency Network

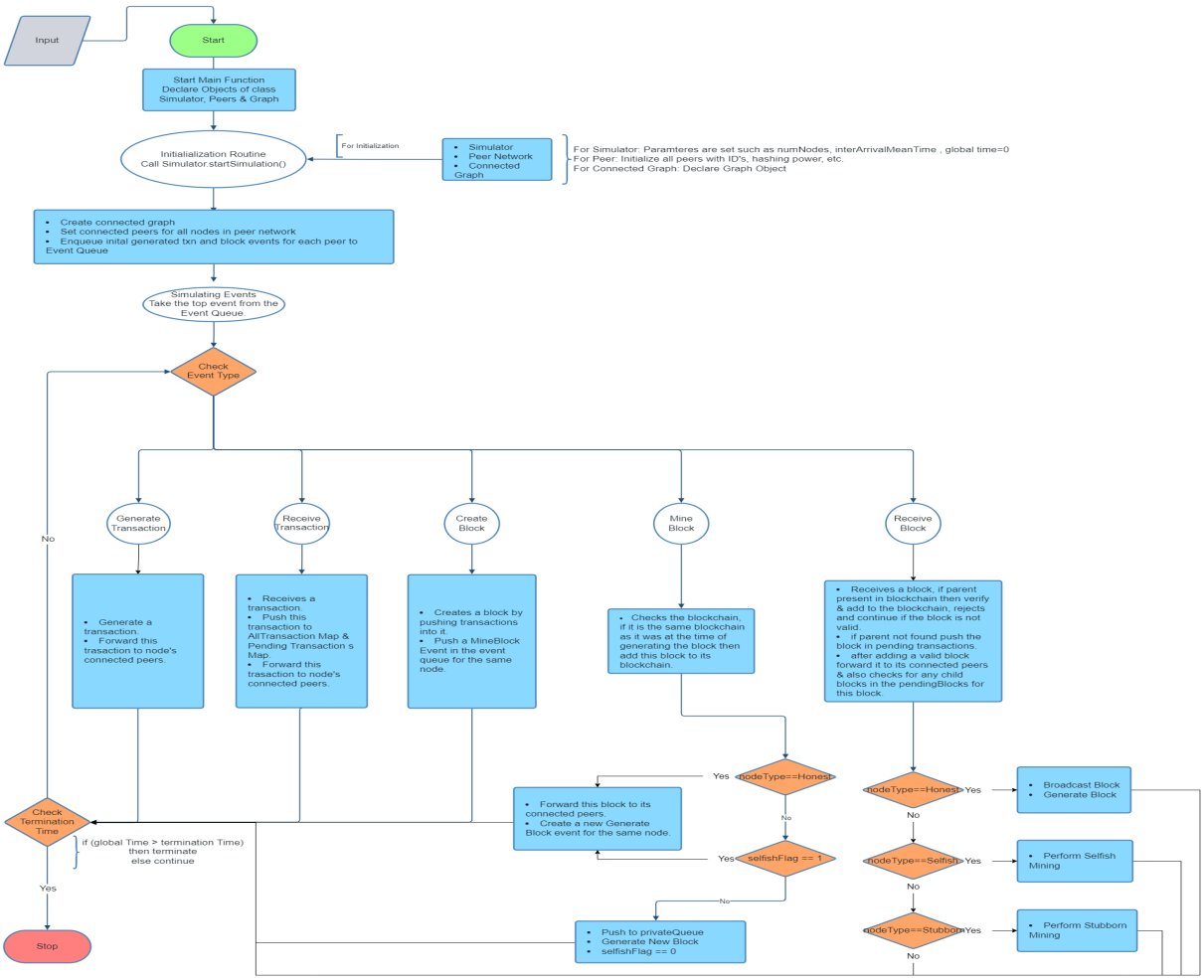
CS 765 : Introduction of Blockchains, Cryptocurrencies, and Smart Contracts
(Project Report)

Jitesh Gawas (22M0748)
Chaitanya Borkar (22M0810)
Mrunal Janbandhu (22M0811)

March, 2023

1 Design Document

Figure 1: Design Document



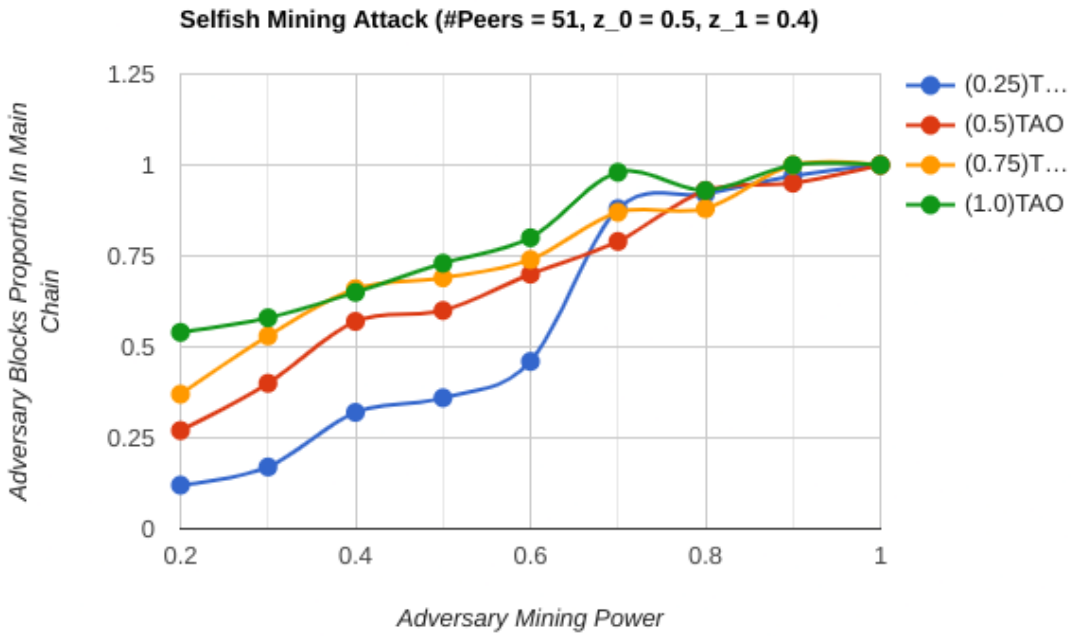
2 Insights and Critiques

In this section, we have provided some insights and critiques on Selfish and stubborn mining that we have simulated on the P2P network. Both concepts refer to mining practices that allow certain miners to gain an unfair advantage over others, potentially leading to centralization and undermining the integrity of the blockchain.

We kept the number of Peers constant at 100 for all the simulation results, and we also maintained constant values of 0.5 and 0.4 for z_0 and z_1, respectively.

2.1 Selfish Mining Attack

Figure 2: Adversary(Selfish) Blocks Proportion In Main Chain



To generate maximum revenue in a Selfish Mining Attack, the percentage of other nodes in the network that the attacker is connected to also plays a crucial role. As depicted in Figure 2, when $\zeta = 0.25$ and the mining power is as high as 0.5, the adversary was able to include around $35 - 40\%$ of the mined blocks in the main chain. However, beyond a certain level of hashing power, the connectivity percentage ζ becomes less significant. Figure 2 shows that when the mining power is above 0.7, the proportion of blocks included in the main chain by the adversary remains within a similar range, irrespective of the value of ζ.

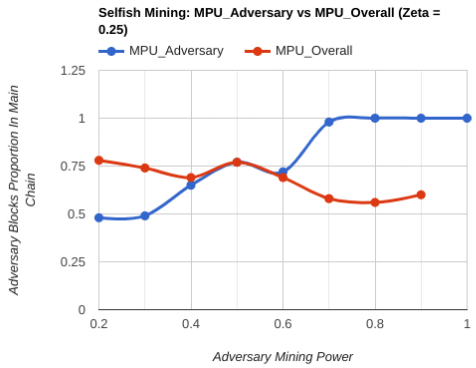


Figure 3: MPU_Ratios : Selfish Mining Attack, $\zeta = 0.25$

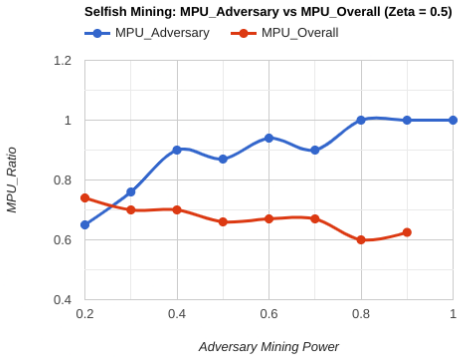
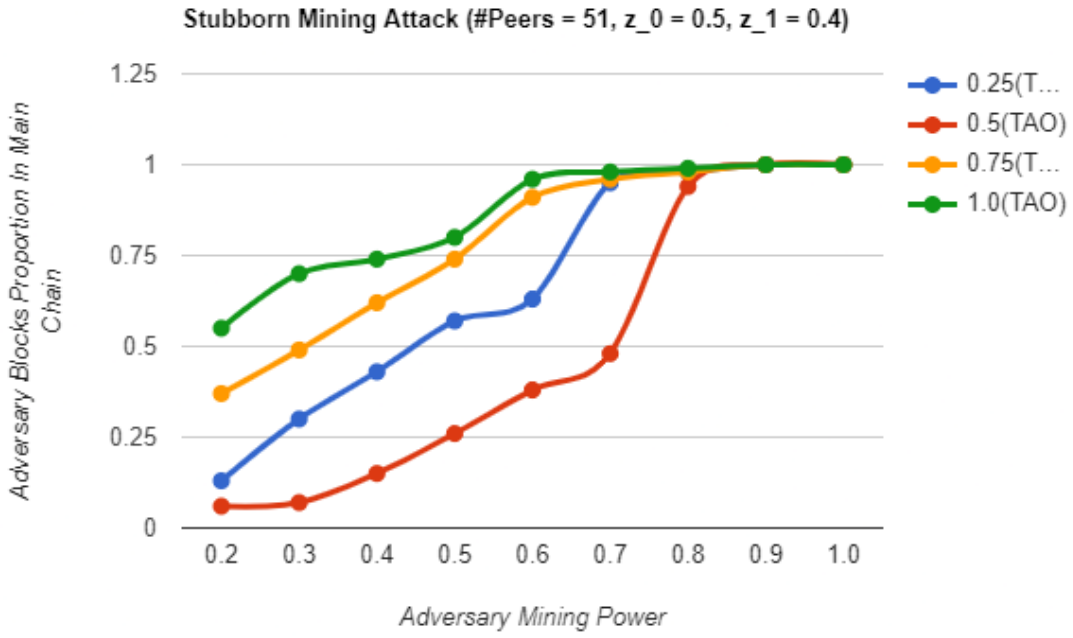


Figure 4: MPU_Ratios : Selfish Mining Attack, $\zeta = 0.5$

From the Figure:3 and Figure:4, It is evident that as the hashing power increases, the MPU_Adversary Ratio approaches 1, indicating that almost all blocks mined by the adversary and sent to other peers are included in the main chain. On the other hand, the MPU_Overall Ratio decreases, indicating a more severe attack, resulting in an increased number of orphaned blocks.

2.2 Stubborn Mining Attack

Figure 5: Stubborn Mining



The maximum revenue generated from a stubborn mining attack exhibits slightly different values, but the trend is somewhat similar to that of the selfish mining attack. In Figure 5, the revenue ratio increases linearly for all values of ζ up to a hashing power of 0.5. As the hashing power increases beyond this threshold, the revenue tends to reach 100%. Furthermore, the significance of connectivity, represented by $\zeta \geq 0.75$, becomes less relevant, as the block proportions are becomes almost identical.

The MPU_Ratios follows a similar trend as what happened with selfish mining attack, from the Figure: 6 and Figure: 7, it is evident that as the hashing power increases the amount of blocks included in the main chain of attacker increases and the overall ratio decreases due to more number of blocks getting orphaned.

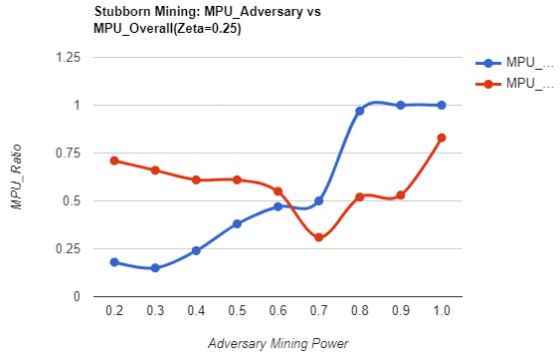


Figure 6: MPU_Ratios : Stubborn Mining Attack, $\zeta = 0.25$

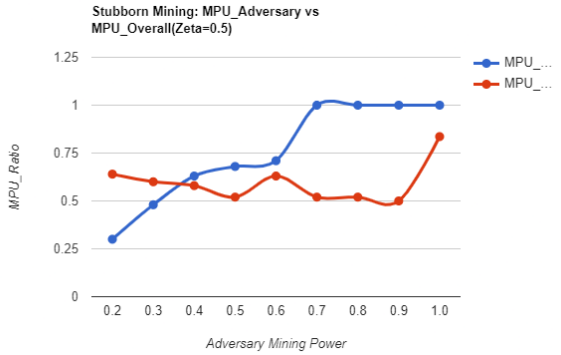


Figure 7: MPU_Ratios : Stubborn Mining Attack, $\zeta = 0.5$