CS765 HW2
Simulating a double selfish mining attack using the P2P Cryptocurrency Network developed in Assignment 1

Magham Dipen Anjan - 210050092
Patil Vipul Sudhir - 210050115
Hari Prakash Reddy - 210050119

March 2024

Terms used to analyse Selfish Mining

$$\mathbf{MPU_{node_{adv}}} = \frac{\text{Number of block mined by an adversary in final public main chain}}{\text{Total number of blocks mined by this adversary overall}}$$

$$\mathbf{MPU_{node_{overall}}} = \frac{\text{Number of block in the final public main chain}}{\text{Total number of blocks generated across all the nodes}}$$

We defined new quantity R_1 as fraction of the fist attacker's blocks in final public chain. Similarly R_2 can defined.

$$\mathbf{R_1} = \frac{\text{Number of block mined by first adversary in final public main chain}}{\text{Number of block in the final public main chain}}$$

Observations

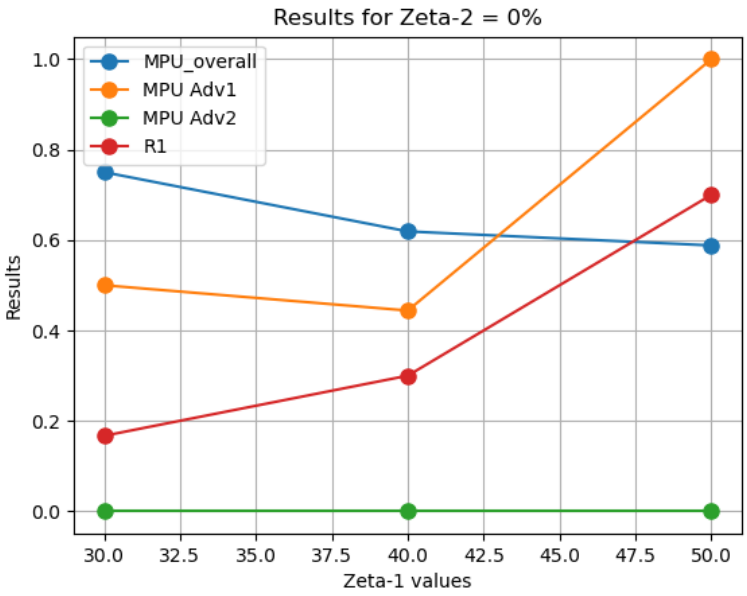
Selfish Mining Simulation Results

Simulation is done using 100 nodes, mean block time 60 seconds, 50% slow honest nodes, with attacker nodes being fast nodes. $\zeta 1$(zeta-1) and $\zeta 2$(zeta-2) denotes mining power of A1 and A2 respectively.

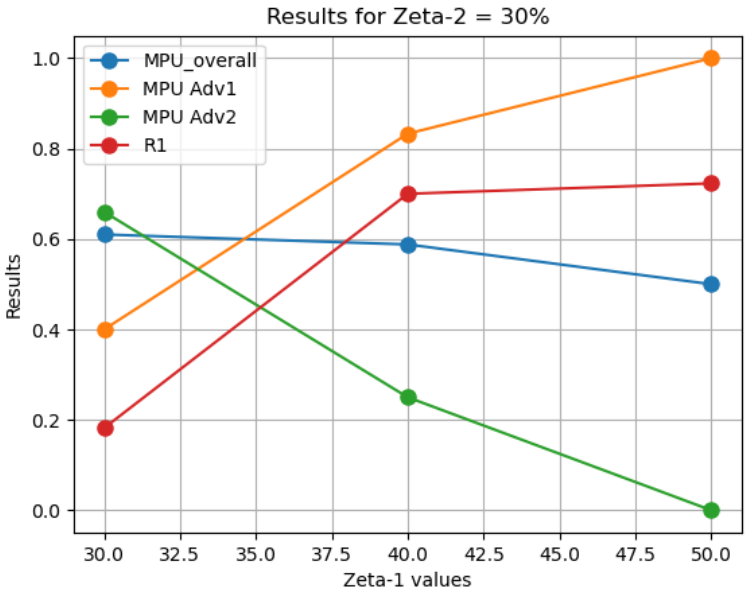
$\zeta 1$	$\zeta 2$	MPU node adv A1	MPU node adv A2	MPU node overall	R1	R2
30	0	0.5	0	0.75	0.1667	0
40	0	0.444	0	0.619	0.30	0
50	0	1	0	0.588	0.7	0
30	30	0.40	0.66	0.61	0.182	0.182
40	30	0.833	0.25	0.588	0.7	0.1
50	30	1	0	0.5	0.723	0
30	45	0	1	0.5833	0	0.92
40	45	0	1	0.56	0	0.95
50	45	1	0	0.82	0.965	0

Varying zeta-1 values

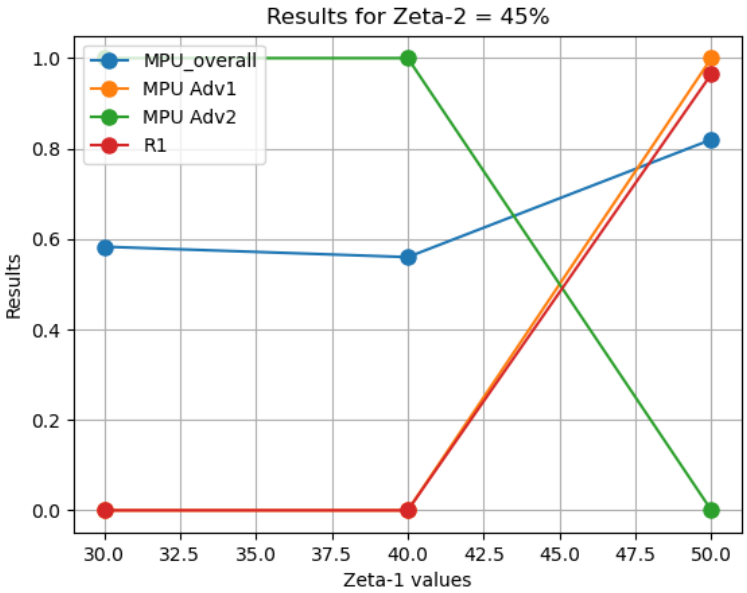
The simulation is done for fixed values of zeta-2 and zeta-1 = 30%, 40%, 50%.



As hashing power of attacker-2 (zeta-2) is zero, we can see it's MPU is also zero. As hashing power of attacker-1 (zeta-1) increases the number of blocks generated by attacker-1 increases so MPU Adv1 and R1 also increases.



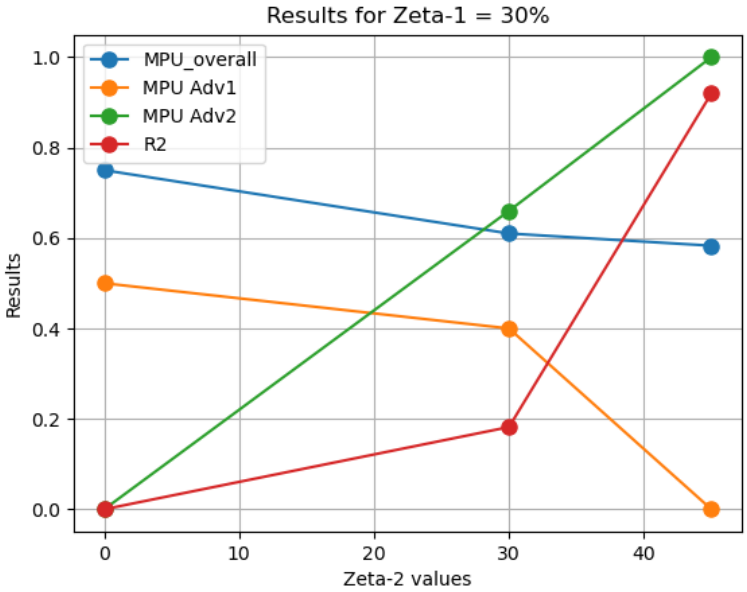
As hashing power of attacker-1 (zeta-1) increases the number of blocks generated by attacker-1 increases so MPU Adv1 and R1 also increases. As attacker-2 has zeta-2 = 30% and zeta-1 increases from 30% to 50%, attacker-1 dominates so MPU Adv2 decreases.



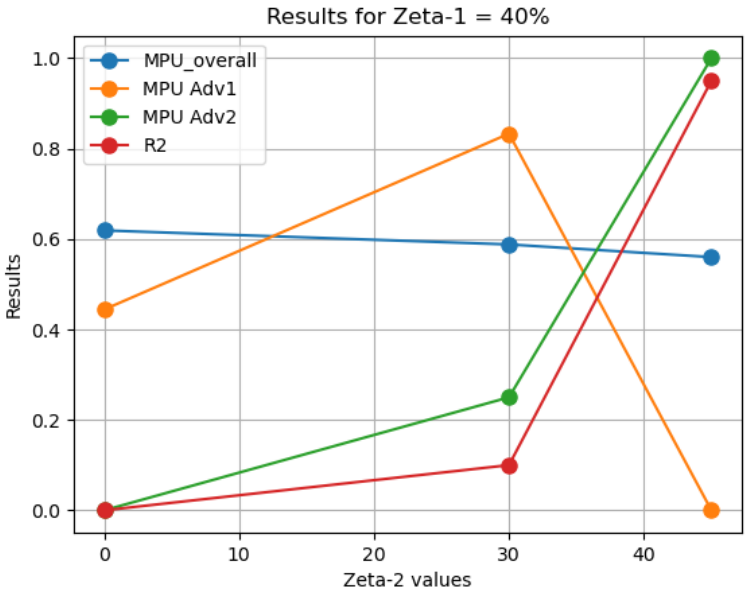
As attacker-2 has zeta-2 = 30% and zeta-1 increases from 30% to 50%, initially attacker-2 dominates so MPU Adv2 is high and when zeta-1 crosses zeta-2 attacker-1 dominates so MPU Adv1 becomes high after the crossing.

Varying zeta-2 values

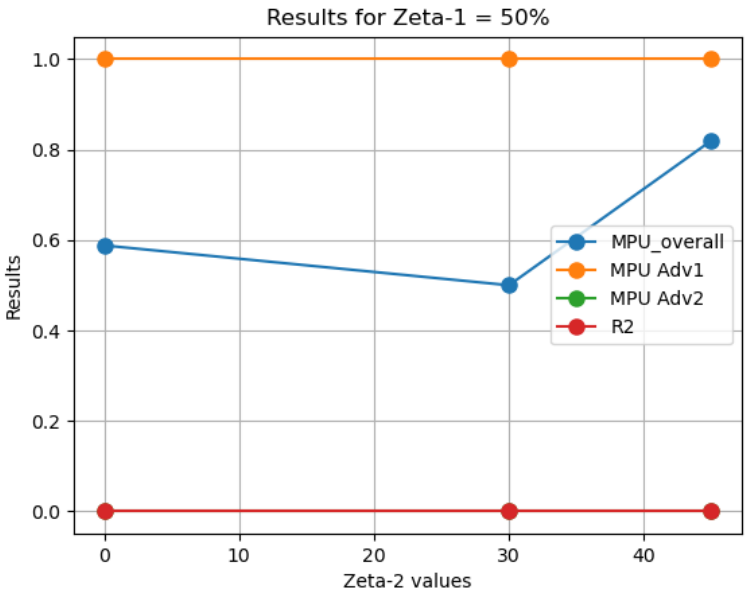
The simulation is done for fixed values of zeta-1 and zeta-2 = 0%, 30%, 45%.



As hashing power of attacker-2 (zeta-2) increases the number of blocks generated by attacker-2 increases, attacker-2 dominates so MPU Adv2 and R2 also increases. As attacker-2 starts dominating MPU Adv1 starts decreasing due to it.



As zeta-1 = 40% and zeta-2 varies from 0% to 45%, initially attacker-1 dominates and after zeta-2 crosses 40% attacker-2 dominates. As attacker-2 starts dominating MPU Adv2 and R2 increases as zeta-2 increases.



As zeta-1 = 50%, Attacker-1 dominates completely so MPU Adv1 = 1, MPU Adv2 and R2 are zero.

Visualization

In visualization we added extra feature which tells whether a specific block is created by Attacker 1 or Attacker 2 or honest nodes. Blocks of Attacker 1 are coloured by ***green***, blocks of Attacker 2 are coloured by ***red*** and remaining ***white*** coloured blocks are created by honest nodes.

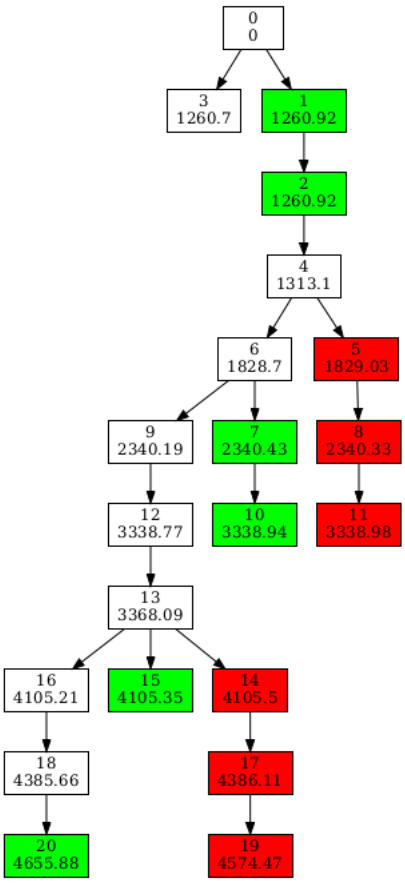


Figure 1: Visualization

Conclusion

1. **Dominance of Blocks in Longest Chain:** The blocks created by the attacker with the most hashing power will dominate the longest chain, as they can create blocks at a faster rate compared to others. In longest chain blocks created by honest nodes will be less.

2. **Lower Attacker Hashing Power and Increased Forking:** When attackers have lower hashing power, forking increases. As they have lower hashing power they struggle to sustain the attack which results into frequent losses.

3. **Impact of Hashing Power Disparity:** Attacker with highest hashing power has more blocks in longest chain as the attacker creates blocks at faster rate which makes other attacker to loose it's private chain.

4. **The Influence of Attacker Node Connectivity on Selfish Mining:** Attacker with higher node connectivity allows attacker to send their mined blocks more effectively to larger group of nodes. So more the connectivity of the attacker with other nodes more the R value.

5. **Power Equality:** If both attackers are equally powerful, they equally share the win. It's like a tie where no one gets ahead.