Simulating a double selfish mining attack using the P2P Cryptocurrency Network

Venkatesh K S, Veeresh B, Vinu Rakav S

March 2024

1 Introduction

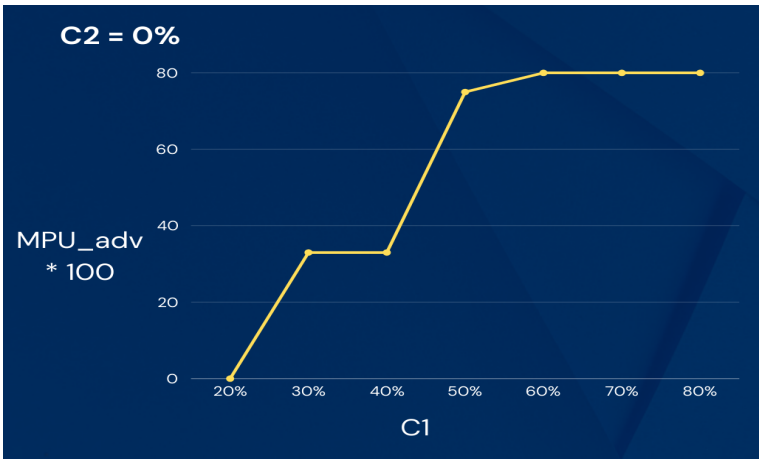
Double Selfish Mining Attack This is the same attack which was proposed by Eyal and Sirer in the paper "Majority is not Enough" with one main difference. In this attack there are two such selfish miners who do not collaborate. Each behaves as if he is the only selfish miner in the system, unaware about the presence of the other attacker.

Honest miner: Each honest node mines on the longest chain visible to it. Tie breaks are resolved according to bitcoin rules, that is in case it sees multiple such longest chains, it mines on the first of these which it sees.

Selfish miner: Each selfish miner considers the longest visible chain (LVC) to him (excluding his current private blocks) as if it were the "honest chain", and tries to selfishly mine as in Eyal and Sirer.

2 Experiment and Analysis

2.1 C2 = 0%



Keeping hashing power of **C2** as 0%, we experimented with different hashing power of **C1** and found out **increase in MPU ratio** of adversary 1 as shown in image above.

Once C2 reaches 50%, a sudden increase in the MPU ratio becomes apparent, consistent with the theoretical explanation. It becomes rare to observe honest blocks being successfully mined during this period.

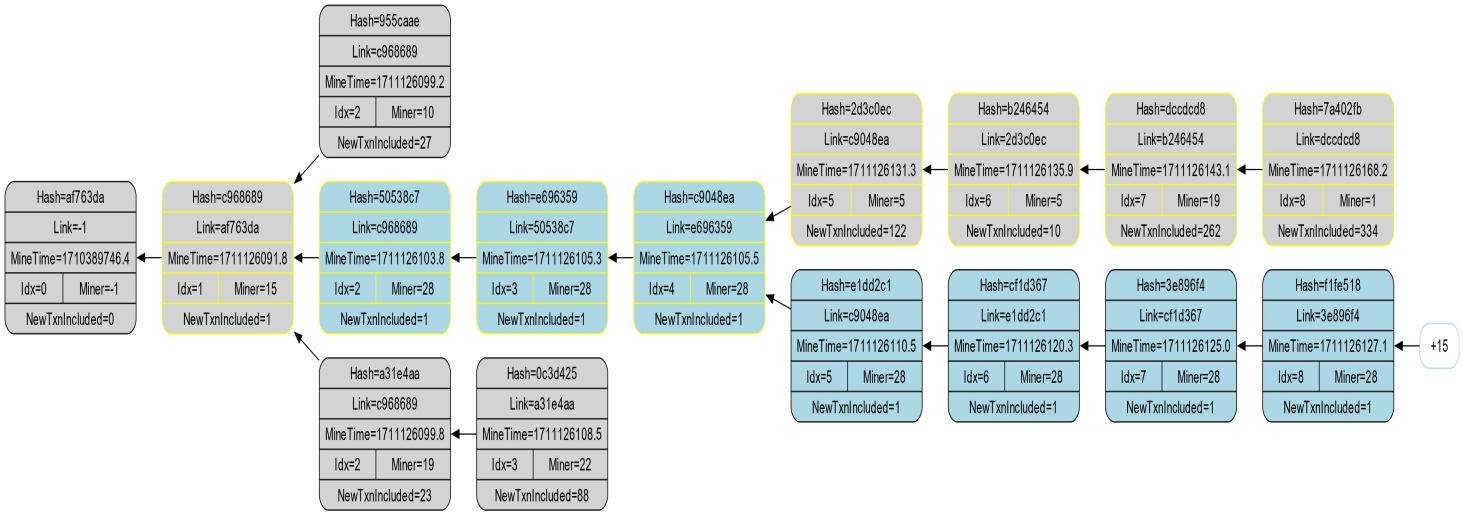


Figure 1: C2 = 40%, C1 = 0%, Adversary = Miner28

From the image provided, it is evident that the selfish miner possesses 15 more blocks privately awaiting the release of blocks from the honest chain in order to cut off their chain.

The table below shows the values of $MPU_{node_{adv}}$ and $MPU_{node_{overall}}$ from a random honest node after a simulation with varying C1 and a fixed C2 at 0%.

h1	20%	30%	40%	50%	60%
h2	0%	0%	0%	0%	0%
MPU_adv	0	0.33	0.33	0.75	0.8
MPU_overall	0.8	0.75	0.56	0.44	0.42

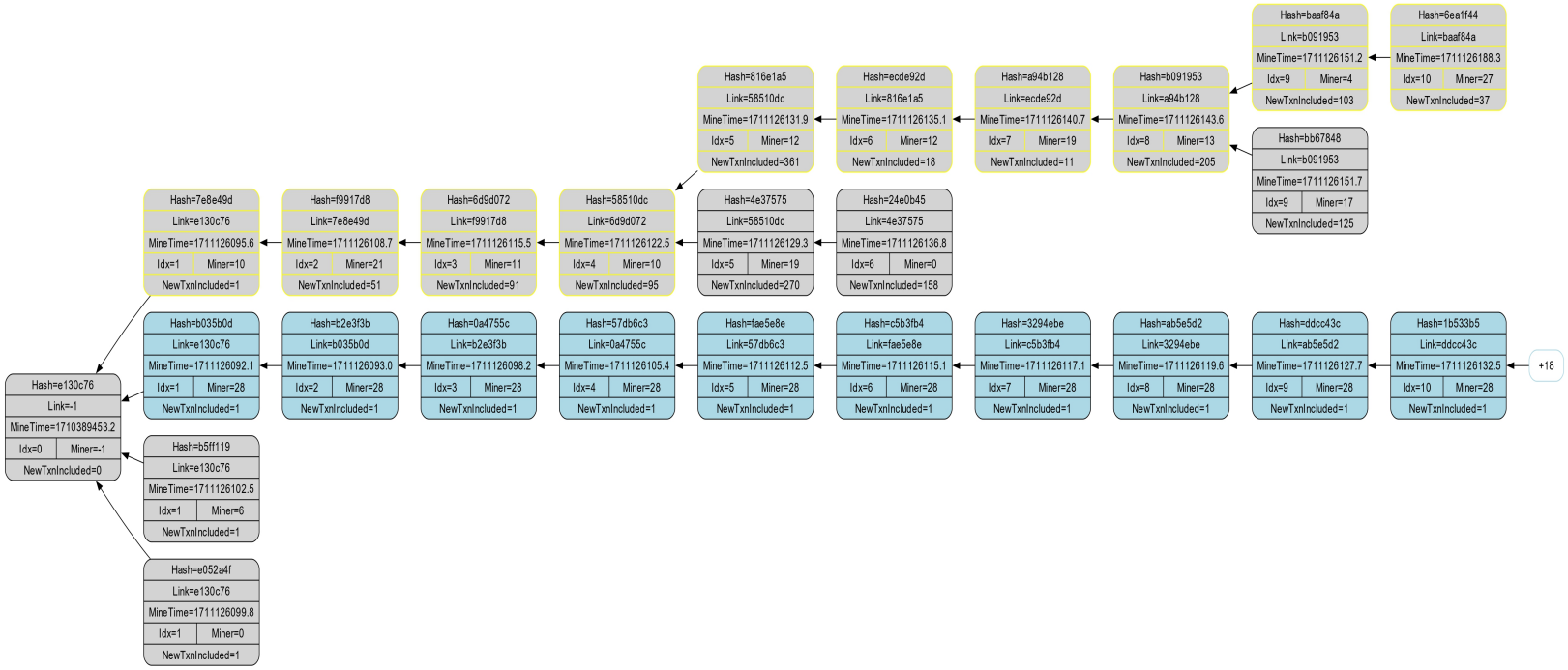
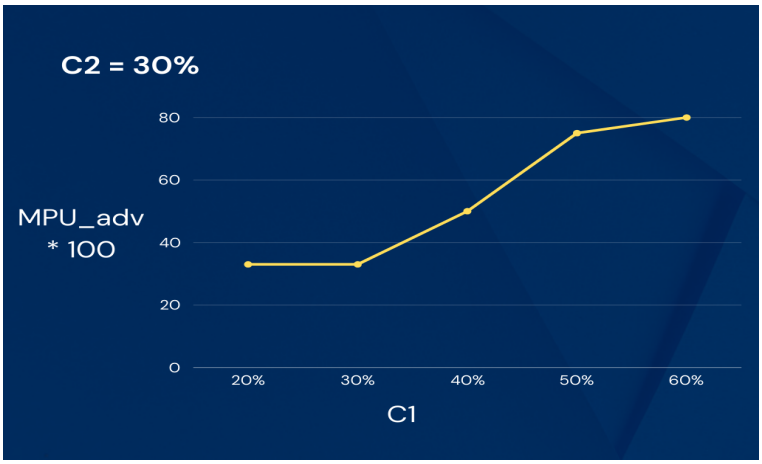


Figure 2: C2 = 60%, C1 = 0%, Adversary = Miner28

It is evident that the adversary has been engaged in an ongoing battle since the beginning, with a total of 18 blocks pending to be used to cut off the main chain.

2.2 C2 = 30%



Keeping hashing power of **C2** as 30%, we experimented with different hashing power of **C1** and found out **increase in MPU ratio** of adversary 1 as shown in image below.

Through our observations, we have noted that as the hashing power increases, the conflict between adversaries intensifies, resulting in the emergence of two longer chains created by each of the adversaries involved in the network.

The following table displays the values of $MPU_{node_{adv}}$ and $MPU_{node_{overall}}$ obtained from a randomly selected honest node after a simulation with varying C1 values, while keeping C2 fixed at 30%.

h1	20%	30%	40%	50%	60%
h2	30%	30%	30%	30%	30%
MPU_adv	0.33	0.33	0.5	0.75	0.8
MPU_overall	0.46	0.35	0.32	0.3	0.3

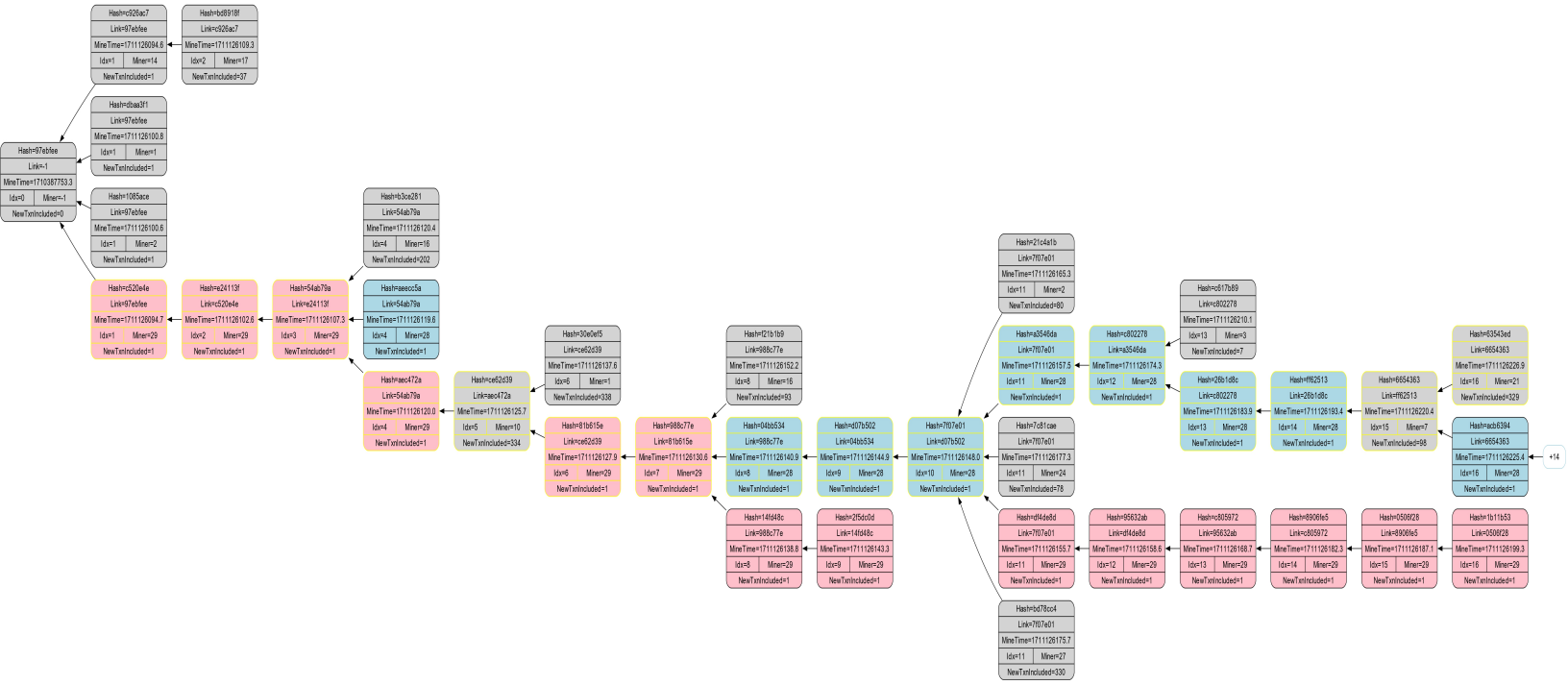


Figure 3: C2 = 20%, C1 = 30%, Adversary = Miner28, Miner29

It is evident from our observations that the adversaries within the network are engaged in conflict with each other, leading to a situation where there are blocks pending release.

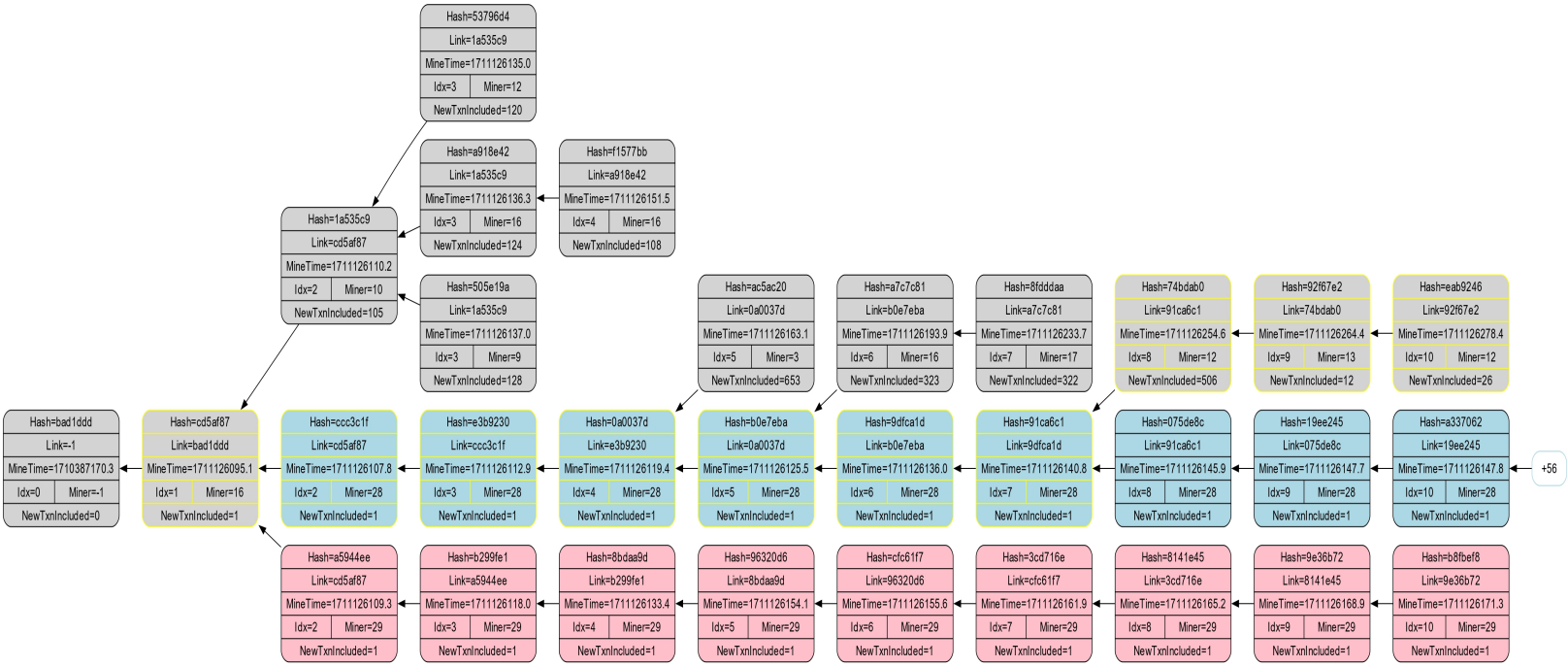


Figure 4: C2 = 40%, C1 = 30%, Adversary = Miner28, Miner29

We can observe that two adversaries are fighting each other, and the whole tree is covered chiefly with adversary blocks.

2.3 Longer run

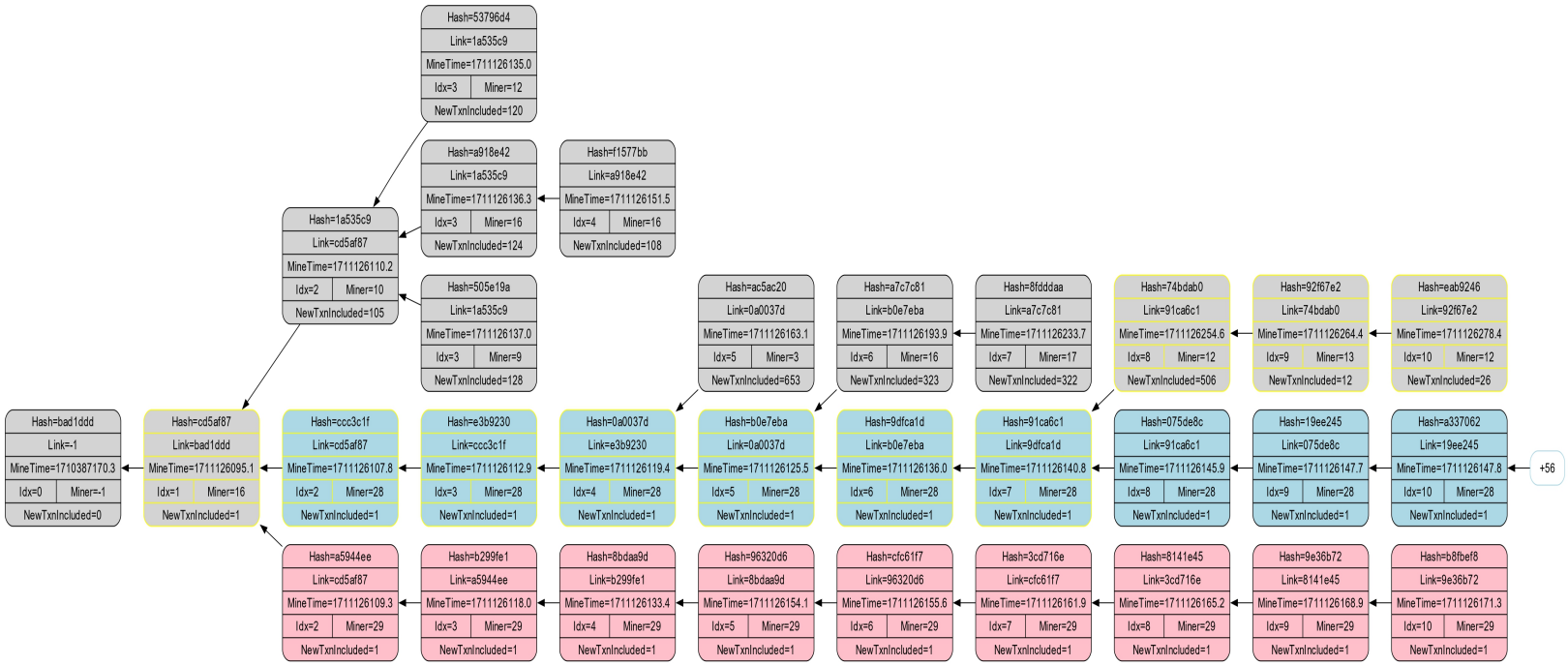


Figure 5: For shorter run, C2 = 40%, C1 = 30%, Adversary = Miner28, Miner29

Utilizing identical parameters and hashing values for the adversaries, we conducted a comparison between a longer run (as shown in the image below) and a shorter run (as depicted in the image above) of the blockchain. It is apparent that the longer run essentially extends from the presence of two elongated chains created by the two adversaries, with a larger number of blocks pending release. This observation leads us to understand that the longer run bears similarities to the shorter run in terms of its structure and pending blocks.

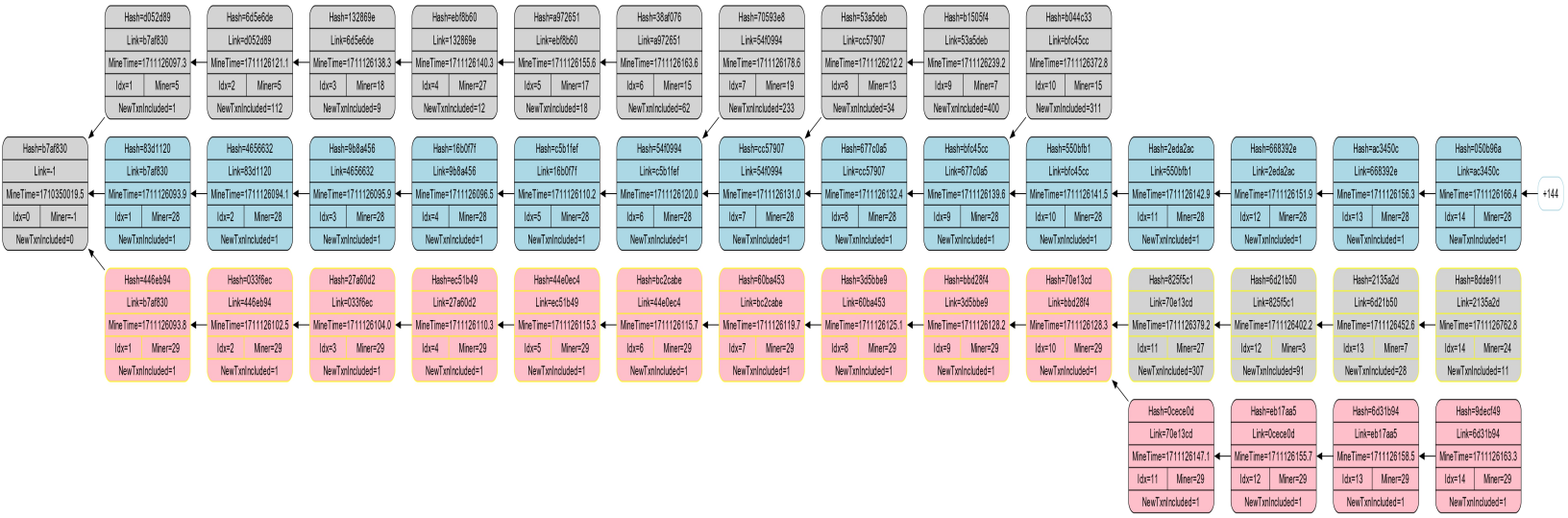


Figure 6: For longer run, C2 = 40%, C1 = 30%, Adversary = Miner28, Miner29

3 Conclusion

- As we increase the hashing power of adversaries, we observe a corresponding increase in the MPU ratio of these adversaries. This heightened MPU ratio creates a situation where Honest Nodes are unable to successfully mine blocks.
- When both adversaries possess higher hashing powers, they engage in conflict, attempting to sever each other's chains.
- When the combined hashing power of the adversaries reaches a higher level, the blockchain is primarily composed of blocks generated by the adversaries.
- With a hashing power of 1, the blockchain consists solely of the Genesis block. This is because honest nodes are unable to mine blocks, and selfish miners do not release blocks.
- Observing $MPU_{node_{overall}}$, we can see in first case of **C2 = 0%** that by increasing C1 values, selfish miners has more power to have alternate chain to honest chain and not release remaining blocks, $MPU_{node_{overall}}$ **saturates to nearby 0.5**.
- In the second case of **C2 = 30%** that by increasing C1 values, both selfish miners fight each other and we can observe two longer chains and one of

them will be the blockchain. There's also honest nodes here and there causing $MPU_{node_{overall}}$ to be **less than 0.5** at all times.

- We have also observed that the chain is similar in both shorter and longer run.