CS765 Project Part-2
Simulation of a P2P Cryptocurrency Network

Sanchit Jindal (200020120), Sarthak Mittal (200050129), Virendra Kabra (200050157)

Spring 2023

Contents

1 Overview

In this Part of the project we build upon the work of Part-1 by also simulating different types of attacks that can be performed in a permission-less block chain. We implement two different types of attacks namely, **Selfish Mining Attack** and the **Stubborn Mining Attack**, We study the affect of different parameters of the block chain and how they affect the working of the attacks

2 Selfish Mining Attack

- This attack was proposed by *Eyal and Sirer* in the paper **Majority is not Enough**
- In this the malicious user does not release its mined blocks immediately, instead it waits till the moment in which it can orphan the most amount of blocks
- This prevents competition for the attacker as the honest nodes waste their resources mining on the block that the attacker is going to orphan
- This also increases the mining fees that the attacker acquires by having a larger percentages of their blocks added to the chain
- The main parameter that is important for the attacker in this attack is the percentage of the total hashing power that he has available for the attack
- Theoretically, with higher percentage of the hashing power the attacker has a higher chance to be able to create a private chain that is longer than the main chain created by the honest nodes and thus higher chance for the attack to succeed

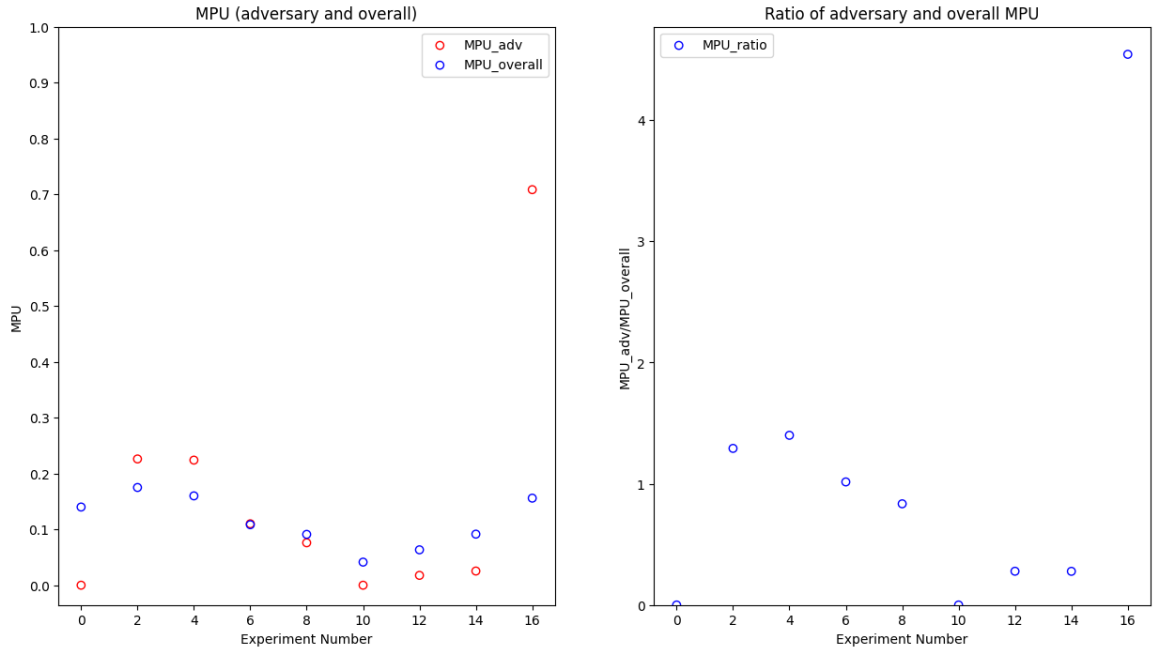

Figure 1: with 30% hashing power

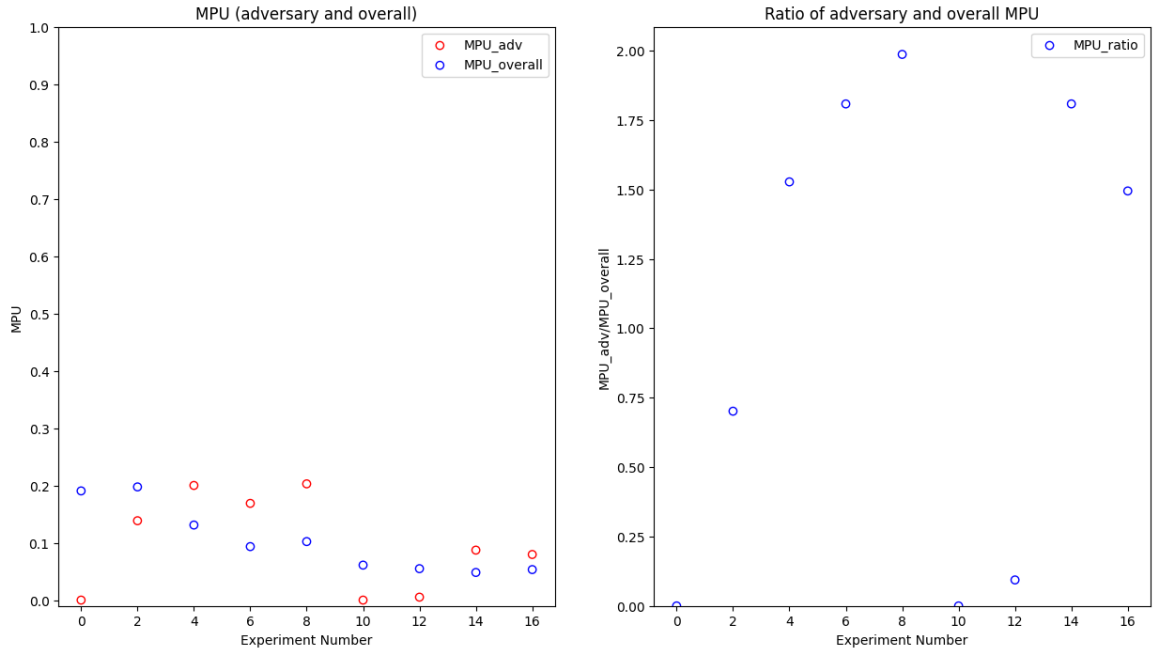

Figure 2: with 50% hashing power

- As it is visible in the plots the **MPU** that is the ratio of the block mined by the attacker in the block chain to the total number of blocks in the blockchain increase drastically as the hashing power of the adversary go from 30% to 50%

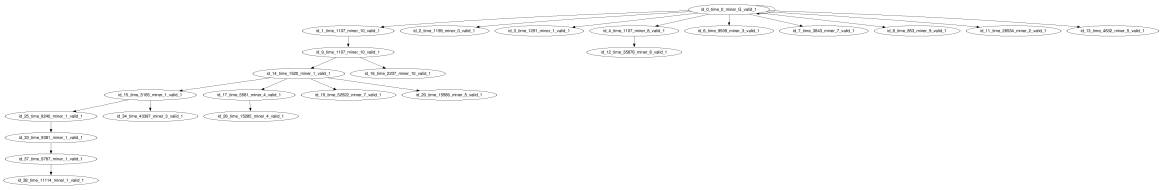

Figure 3: lock Chain of honest miner

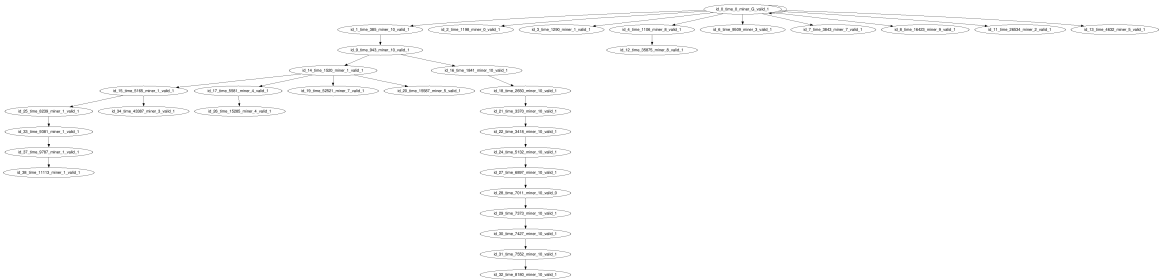

Figure 4: Block Chain of attacker

- The Attacker keeps a large chain of unreleased blocks private that are released as soon as the honest nodes are going to catch up, this orphans the honest nodes blocks and the attack succeeds

3 Stubborn Mining Attack

- This is a variation of the Selfish Mining Attack in which the malicious user does not release the whole private chain when the honest chain is about catch up

- instead the attacker only releases one node at a time to maintain a lead for the longest time possible
- This increases the duration of the attack as in selfish mining attack once the chain is released the attack finishes and the attackers lead goes to zero as all the nodes start mining on the latest block but in this the attacker presents a block to for the nodes to mine on which he will later orphan thus continuing his attack
- In this attack also the Hashing Percentage is a important parameter for the probability of the attack to succeed as a higher hashing power means that there is a higher probability for the attacker to mine and collect multiple blocks

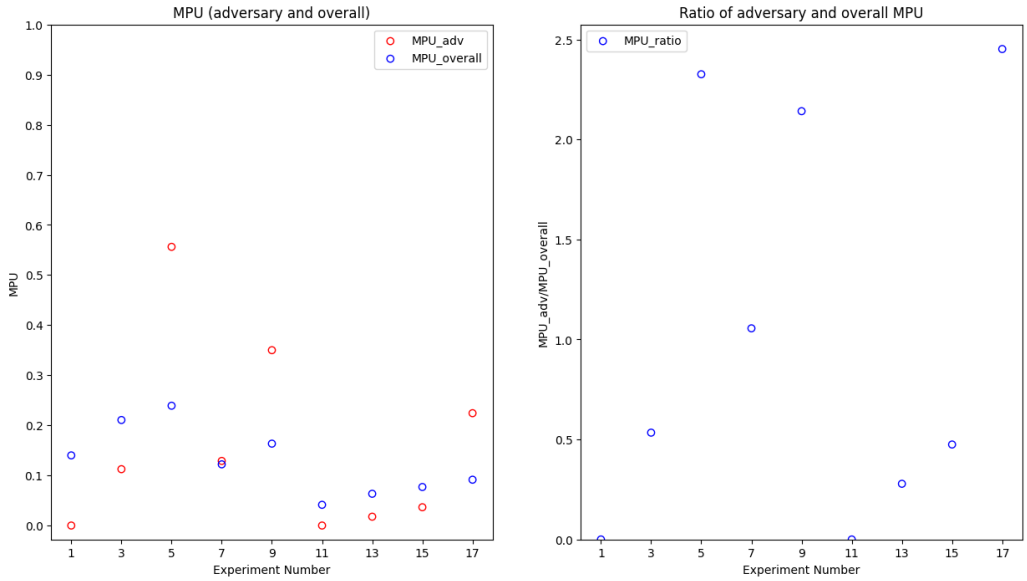

Figure 5: with 30% hashing power

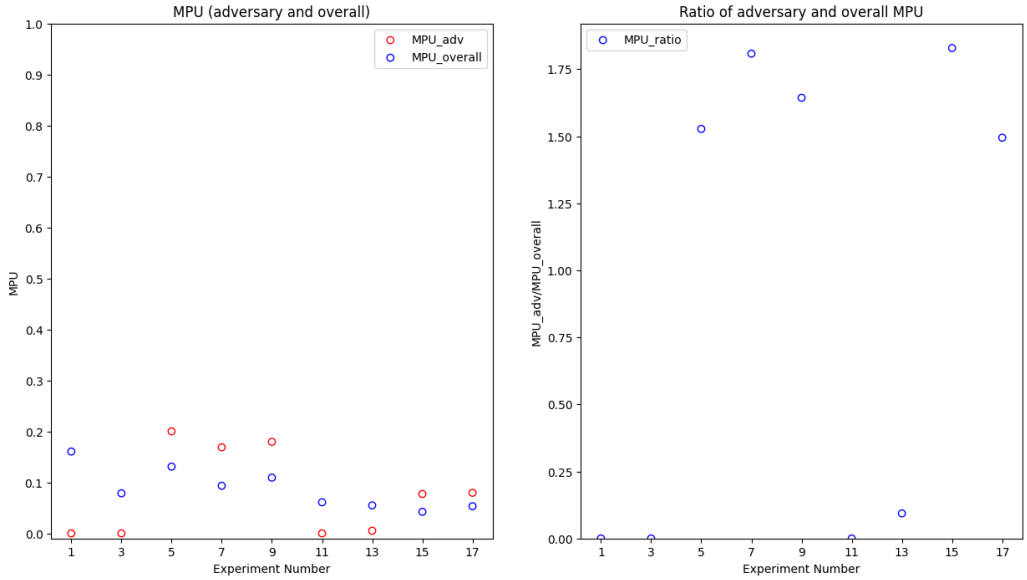

Figure 6: with 50% hashing power

- As is visible in the plots when the attacker has 50% hashing power then the **MPU** value is higher for more experiments than for the 30%hashing power case