# Blockchain and Cryptocurrencies

A2 - Mining Attacks

Anubhav (180050010), Rishi (180050086)

October 2021

## 1 Experiments and Discussion

The parameters for the experiment are:

- Hashing fraction of the adversary (denoted by $adv$)
- Fraction of nodes connected to the adversary (denoted by $\zeta$)
- The type of adversary - either selfish miner or stubborn miner.

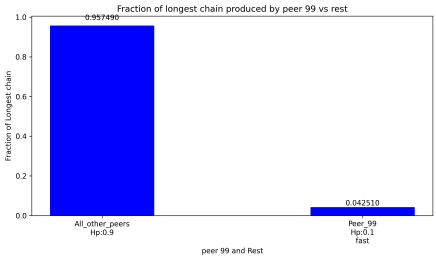
In all the experiments we set the number of peers to 100. We let the simulation continue till we generate roughly 500 blocks. We run 24 different types of experiments:

- Selfish miner with $adv \in \{10\%, 20\%, 35\%, 50\%\}$ and $\zeta \in \{25\%, 50\%, 75\%\}$
- Stubborn miner with $adv \in \{10\%, 20\%, 35\%, 50\%\}$ and $\zeta \in \{25\%, 50\%, 75\%\}$

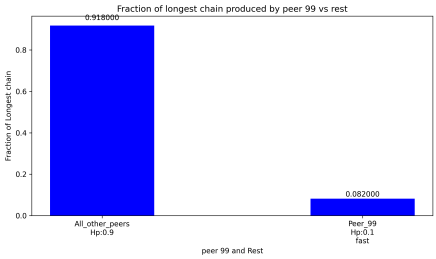
We observe from figures (1, 3) that stubborn mining performs similar to selfish mining for most values of $\zeta$ and $adv$. However, for $\zeta = 25\%$, $adv = 35\%$ we observe that stubborn mining outperforms selfish mining. This implies that stubborn mining might start giving benefits earlier as compared to selfish mining, however, the difference soon tapers off.

We further observe from figures (2, 4) that on increasing the fraction of hashing power ($adv$) of an attacker (both selfish and stubborn), the $MPU_{overall}$ and $MPU_{honest}$ reduce, while $MPU_{attacker}$ increases. Furthermore, figures (1, 3) show that fraction of chain controlled by the attacker increases manifolds as $adv$ increases. This is in line with the theoretical results by [1]

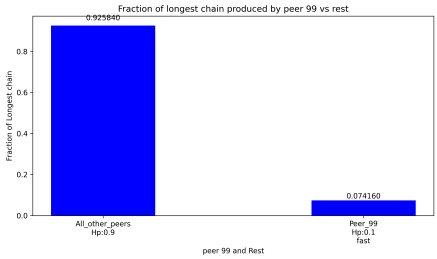
From figures (1, 3) we observe that $\zeta$ plays an important role for especially smaller values of $adv$. For example, for $adv = 10\%$ a selfish attacker suffers alot when $\zeta = 25\%$, however, the attacker suffers less when $\zeta$ increases to 50% and 75%. On the other hand, for larger values of $adv$, $\zeta$ does not play a very crucial role. This is also in line with the theoretical results by [1].



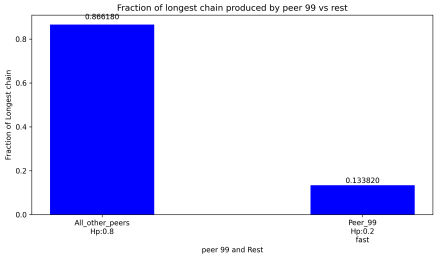

(a) $\zeta = 25\%$, $adv = 10\%$



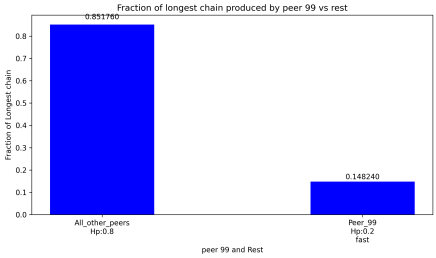

(b) $\zeta = 50\%$, $adv = 10\%$



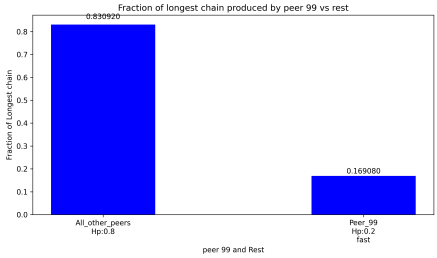

(c) $\zeta = 75\%$, $adv = 10\%$



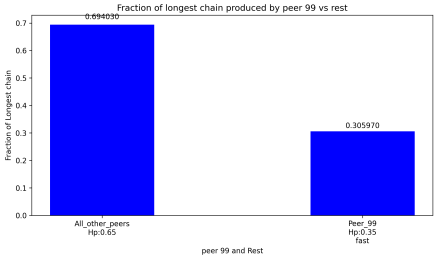

(d) $\zeta = 25\%$, $adv = 20\%$



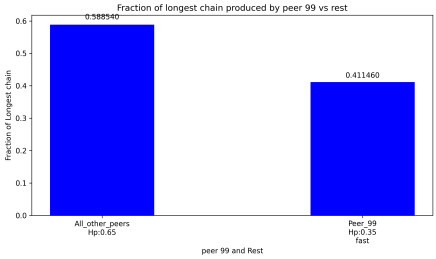

(e) $\zeta = 50\%$, $adv = 20\%$



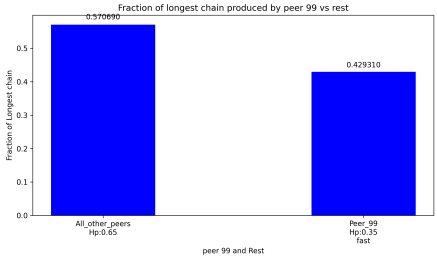

(f) $\zeta = 75\%$, $adv = 20\%$



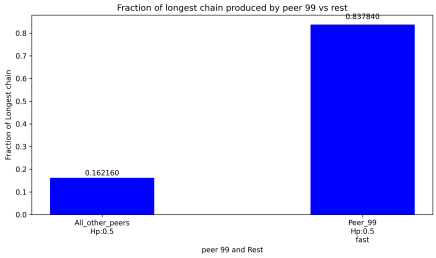

(g) $\zeta = 25\%$, $adv = 35\%$



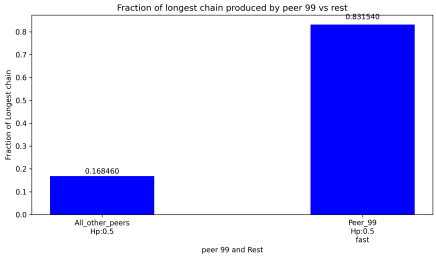

(h) $\zeta = 50\%$, $adv = 35\%$



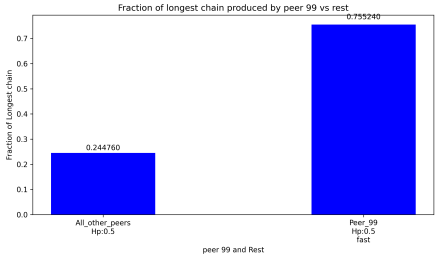

(i) $\zeta = 75\%$, $adv = 35\%$




(j) $\zeta = 25\%$, $adv = 50\%$

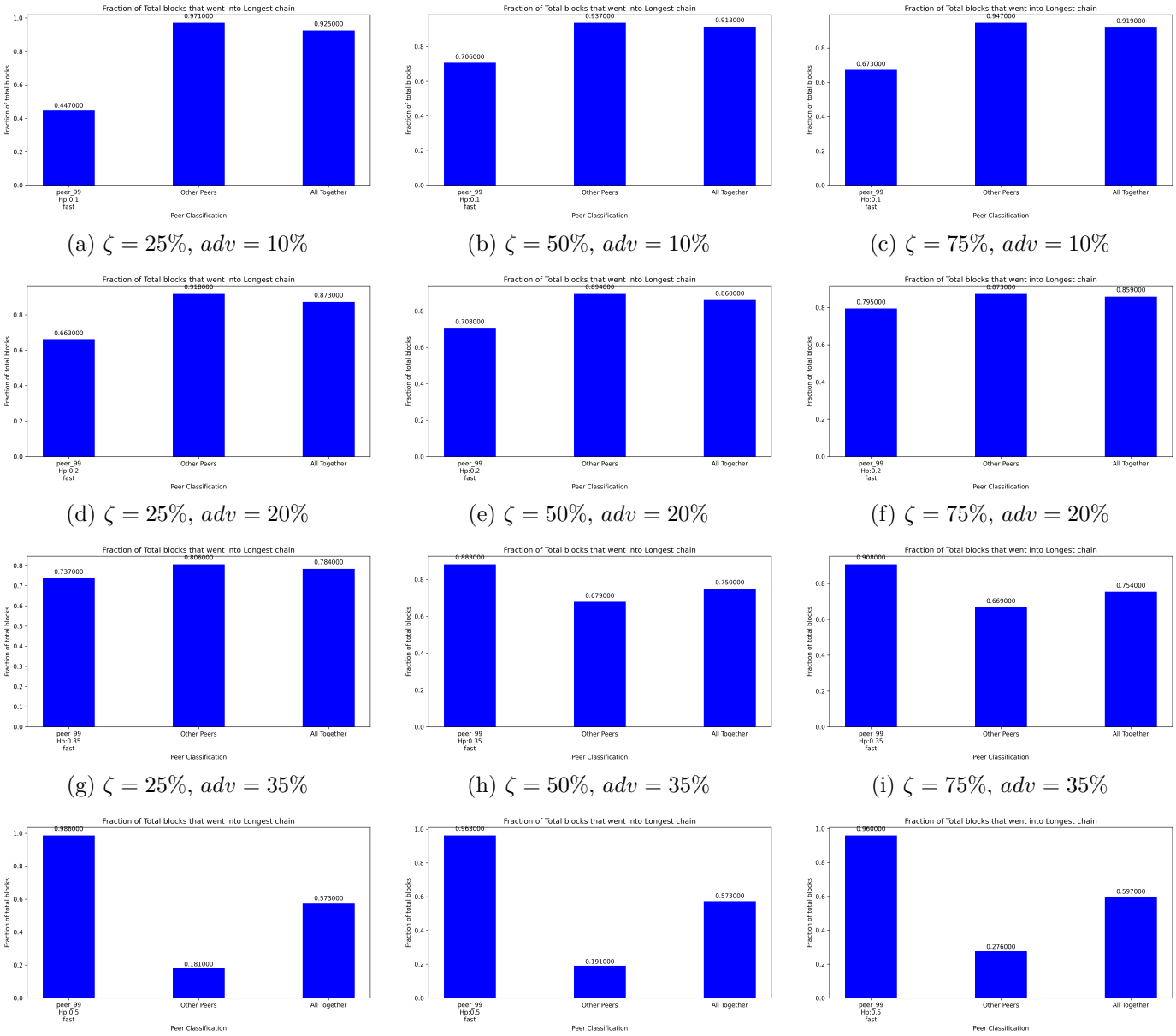



(k) $\zeta = 50\%$, $adv = 50\%$




(l) $\zeta = 75\%$, $adv = 50\%$

Figure 1: Fraction of blocks generated in the longest chain by the honest miners collectively (first bar in the graphs) vs a **selfish miner** (second bar in the graphs). We vary $\zeta$ across each row from 25% to 75%, and $adv$ across each column from 10% to 50%.



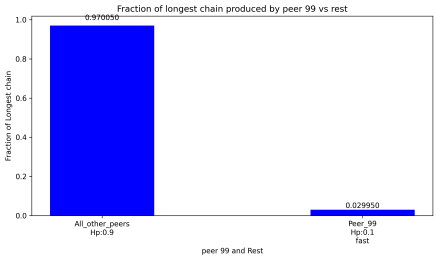

(a) $\zeta = 25\%$, $adv = 10\%$ (b) $\zeta = 50\%$, $adv = 10\%$ (c) $\zeta = 75\%$, $adv = 10\%$

(d) $\zeta = 25\%$, $adv = 20\%$ (e) $\zeta = 50\%$, $adv = 20\%$ (f) $\zeta = 75\%$, $adv = 20\%$

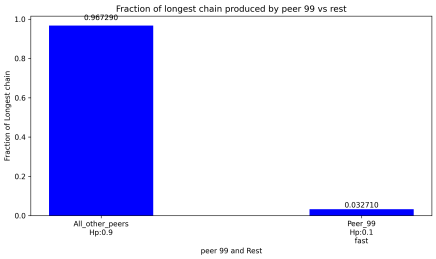
(g) $\zeta = 25\%$, $adv = 35\%$ (h) $\zeta = 50\%$, $adv = 35\%$ (i) $\zeta = 75\%$, $adv = 35\%$

(j) $\zeta = 25\%$, $adv = 50\%$ (k) $\zeta = 50\%$, $adv = 50\%$ (l) $\zeta = 75\%$, $adv = 50\%$

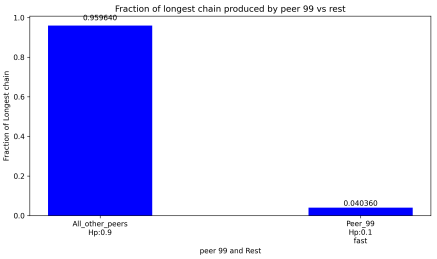
Figure 2: MPU for the selfish miner (first bar), honest miners collectively (second bar) and overall (third bar). We vary $\zeta$ across each row from 25% to 75%, and $adv$ across each column from 10% to 50%.



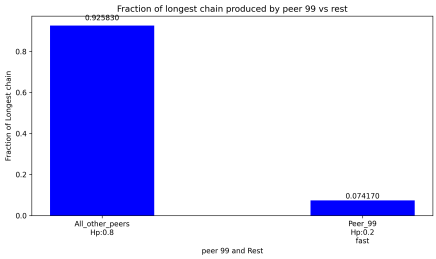

(a) $\zeta = 25\%$, $adv = 10\%$



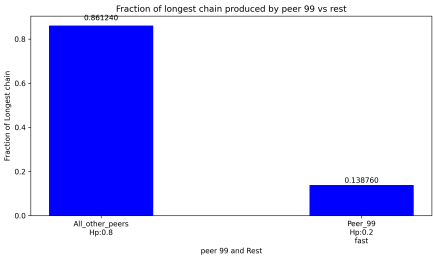

(b) $\zeta = 50\%$, $adv = 10\%$



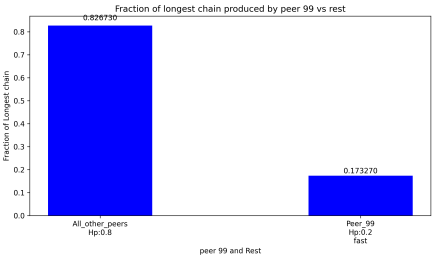

(c) $\zeta = 75\%$, $adv = 10\%$



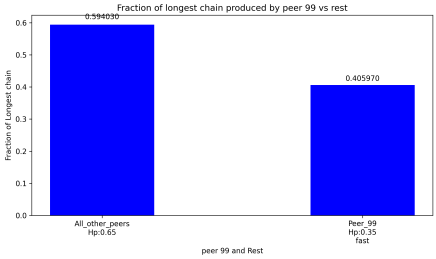

(d) $\zeta = 25\%$, $adv = 20\%$



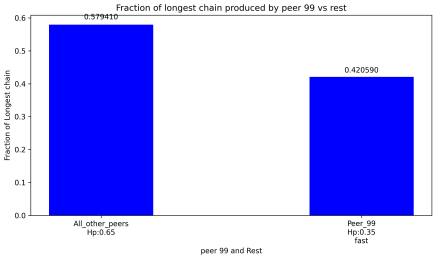

(e) $\zeta = 50\%$, $adv = 20\%$



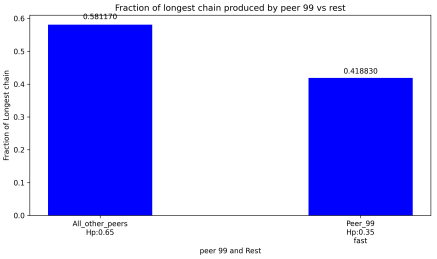

(f) $\zeta = 75\%$, $adv = 20\%$



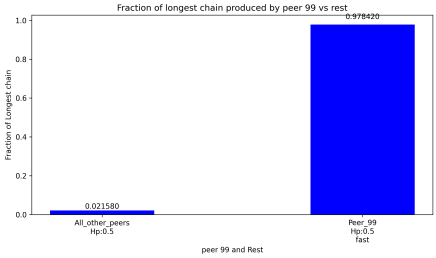

(g) $\zeta = 25\%$, $adv = 35\%$



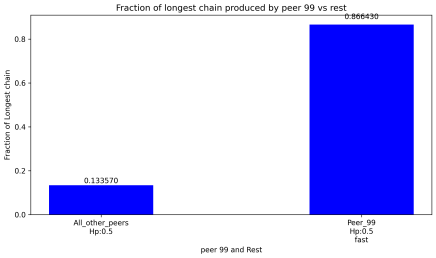

(h) $\zeta = 50\%$, $adv = 35\%$



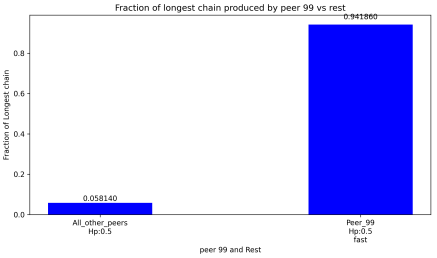

(i) $\zeta = 75\%$, $adv = 35\%$




(j) $\zeta = 25\%$, $adv = 50\%$

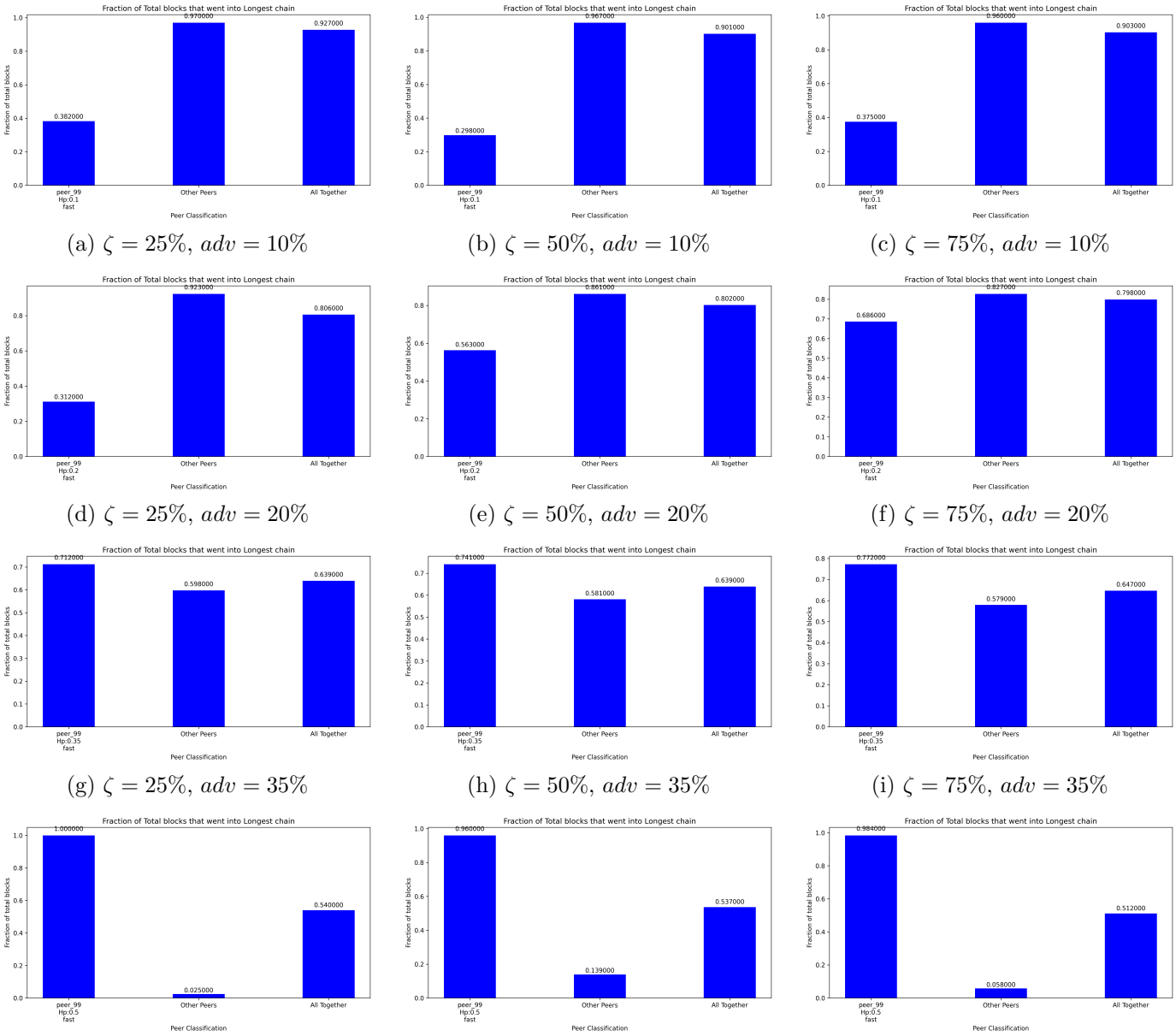



(k) $\zeta = 50\%$, $adv = 50\%$




(l) $\zeta = 75\%$, $adv = 50\%$

Figure 3: Fraction of blocks generated in the longest chain by the honest miners collectively (first bar in the graphs) vs a **stubborn miner** (second bar in the graphs). We vary $\zeta$ across each row from 25% to 75%, and $adv$ across each column from 10% to 50%.




(a) $\zeta = 25\%$, $adv = 10\%$ (b) $\zeta = 50\%$, $adv = 10\%$ (c) $\zeta = 75\%$, $adv = 10\%$

(d) $\zeta = 25\%$, $adv = 20\%$ (e) $\zeta = 50\%$, $adv = 20\%$ (f) $\zeta = 75\%$, $adv = 20\%$

(g) $\zeta = 25\%$, $adv = 35\%$ (h) $\zeta = 50\%$, $adv = 35\%$ (i) $\zeta = 75\%$, $adv = 35\%$

(j) $\zeta = 25\%$, $adv = 50\%$ (k) $\zeta = 50\%$, $adv = 50\%$ (l) $\zeta = 75\%$, $adv = 50\%$

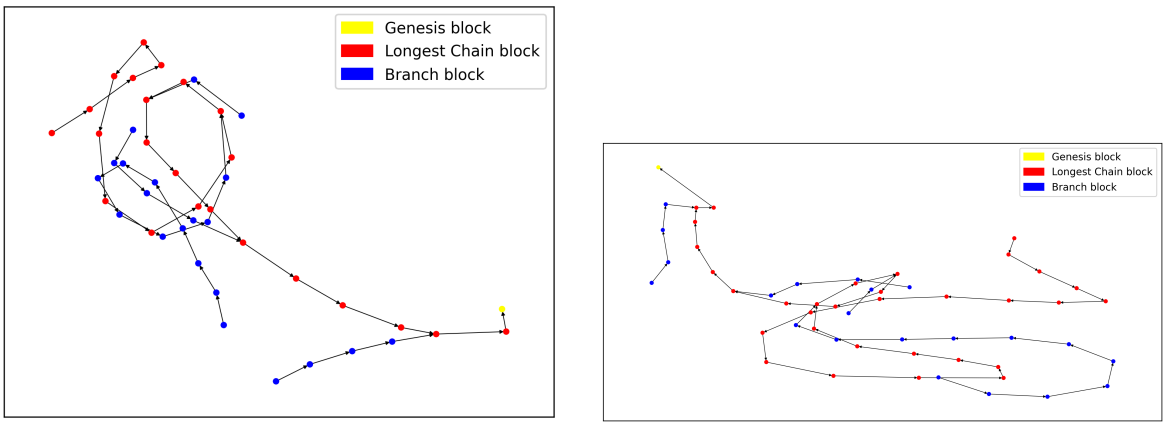
Figure 4: MPU for the stubborn miner (first bar), honest miners collectively (second bar) and overall (third bar). We vary $\zeta$ across each row from 25% to 75%, and $adv$ across each column from 10% to 50%.

Now lets compare our simulation results from figure (1) with the theoretical estimates given by [1].

| | $\zeta = 25\%$ | | $\zeta = 50\%$ | | $\zeta = 75\%$ | |
|---|---|---|---|---|---|---|
| | Theoretical | Simulation | Theoretical | Simulation | Theoretical | Simulation |
| **adv = 10%** | 0.05 | 0.04 | 0.07 | 0.08 | 0.09 | 0.07 |
| **adv = 20%** | 0.16 | 0.14 | 0.18 | 0.15 | 0.21 | 0.17 |
| **adv = 35%** | 0.39 | 0.31 | 0.42 | 0.42 | 0.44 | 0.43 |
| **adv = 50%** | 1.00 | 0.84 | 1.00 | 0.83 | 1.00 | 0.76 |

Table 1: Comparison between theoretical results and simulation results for chain fraction of a selfish miner over different values of $\zeta$ and *adv*

We show the blockchains as perceived by an honest miner and a selfish miner for $\zeta = 25\%$, $adv = 50\%$ next.




(a) As seen by an honest miner

(b) As seen by a selfish miner

Figure 5: Blockchains as perceived by an honest miner and a selfish miner for $\zeta = 25\%$, $adv = 50\%$

We observe the presence of blue blocks which indicate presence of branches. This is expected as the selfish miner maintains private chains which will lead to branching. Furthermore, we observe that the number of blocks in the selfish miner's tree is more than that in the honest miner's tree. This indicates that the selfish miner has a longer private chain which he has not released.

# References

[1] Ittay Eyal and Emin Gun Sirer. *Majority is not Enough: Bitcoin Mining is Vulnerable*. 2013. arXiv: `1311.0243 [cs.CR]`.