CS765 - INTRODUCTION TO BLOCKCHAINS, CRYPTOCURRENCIES AND SMART CONTRACTS

Report on Simulating a selfish mining attack on a P2P Cryptocurrency Network

CHIRANMOY BHATTACHARYA
22M0744

SAI KUMAR ATLURI
22M0745

HEMANTH NARADASU
22M0777

Simulation Parameters

The simulation was run for varying values of adversary hashing power (alpha), and the fraction of honest miners an adversary is connected to (zeta). Other parameters were fixed to the following values.

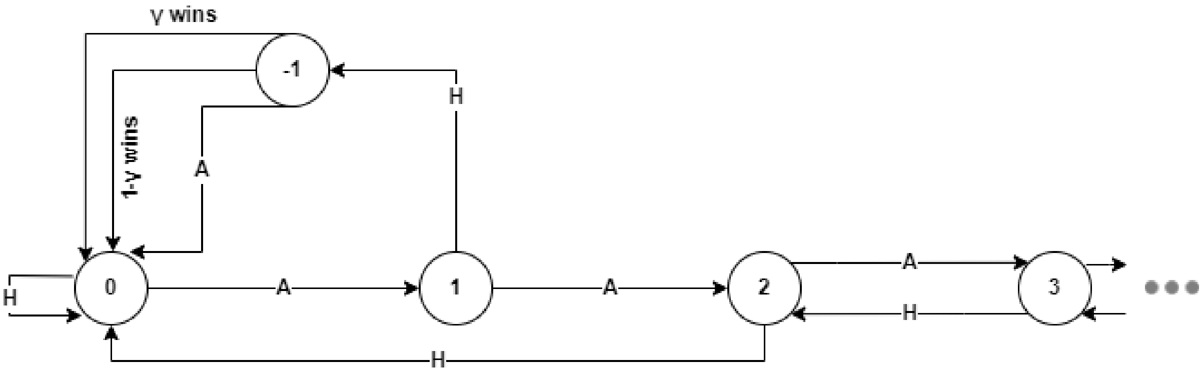
Number of miners (n) = 100
Percent of Fast CPU Miners (z_0) = 50
Percent of Fast Link Miners (z_1) = 50
Block Inter-arrival time (t_{blk}) = 600 (in seconds)
Meantime, to generate a transaction (t_{txn}) = 1000000 (in seconds)
Number of events to simulate (eventCount) = 750000

The mean time to generate a transaction (t_{txn}) is kept high to focus on block generation.

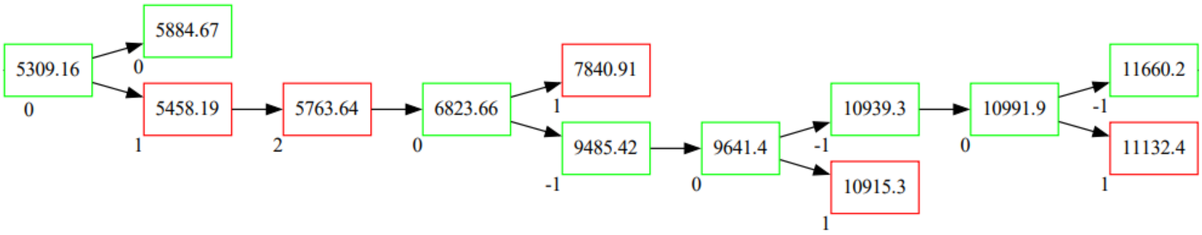
Selfish Mining Attack

A selfish mining attack is a strategy in which a dishonest miner or a group of miners deliberately withhold the discovery of new blocks from the network, creating an unfair advantage over other miners. Instead of immediately broadcasting the new block to the network, selfish miners keep the block private and continue to work on the next block. This allows them to build a longer chain than the rest of the network and increases their chances of winning the block reward. The private chain is then released at an opportune moment, orphaning the honest miner’s main chain.

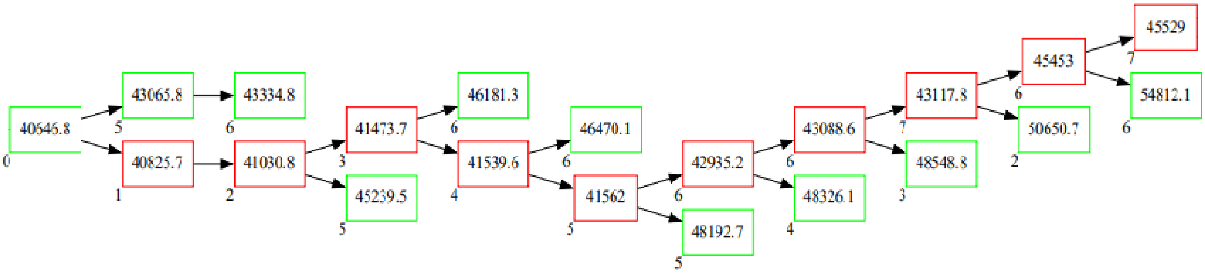
State Diagram of Selfish Miner



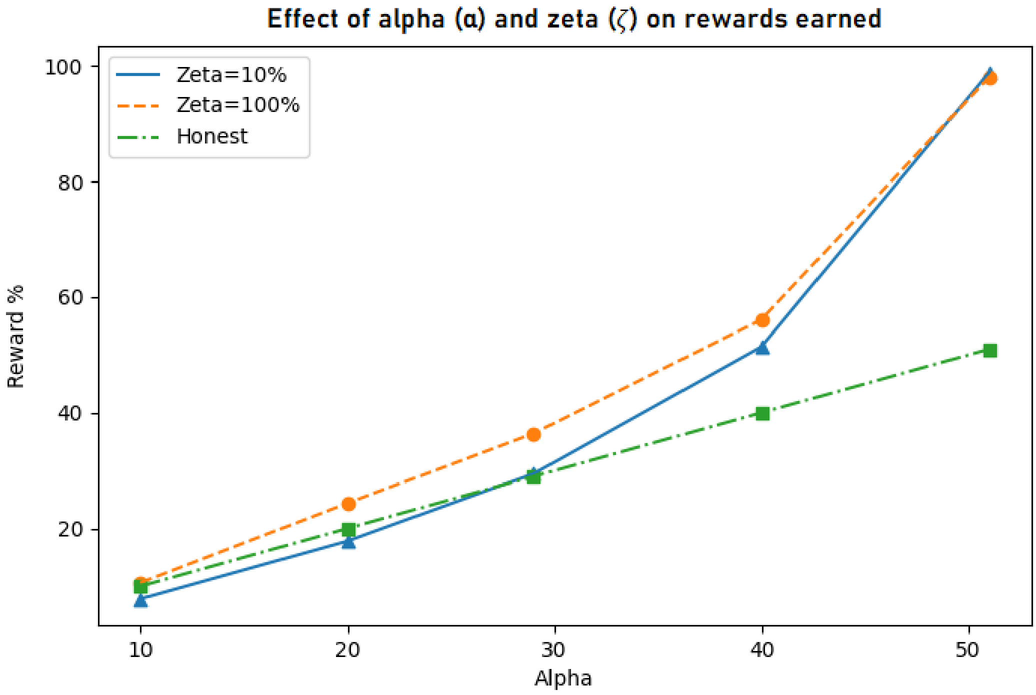
Example blockchain tree with parameters alpha = 20 and zeta = 20



Example blockchain tree with parameters alpha = 40 and zeta = 20



Effect of selfish miner's hashing power (Alpha) and network connectivity (Zeta) on rewards earned



In the above graph, the x-axis represents the adversary miner's hashing power alpha (**α**), and the y-axis represents the rewards earned by the adversary. We take the attacker's network connectivity as zeta(ζ) and draw a line graph with the assumption that zeta is constant; the orange line has maximum connectivity, i.e., the attacker is connected to all miners in the network, and the blue line has a zeta value of 10%, i.e., the attacker is connected to 10% of the honest nodes in the network.

1. **Miner is honest**
   If the miner is honest, then the reward earned by the miner is equal to its fraction of hashing power.

2. **Zeta (ζ) = 100%, and the adversary performs selfish mining**
   The orange line in the graph clearly depicts that the hashing power of the attacker doesn't matter when the attacker has the maximum connectivity. Performing selfish mining always results in higher rewards than being an honest miner. This is because when zeta(ζ) is the maximum, the adversary is connected to all honest miners in the network, then the gama (γ), which represents the percentage of honest miners mining the attacker's block, also be at maximum, this increases the probability of attacker chain to win at state(0').

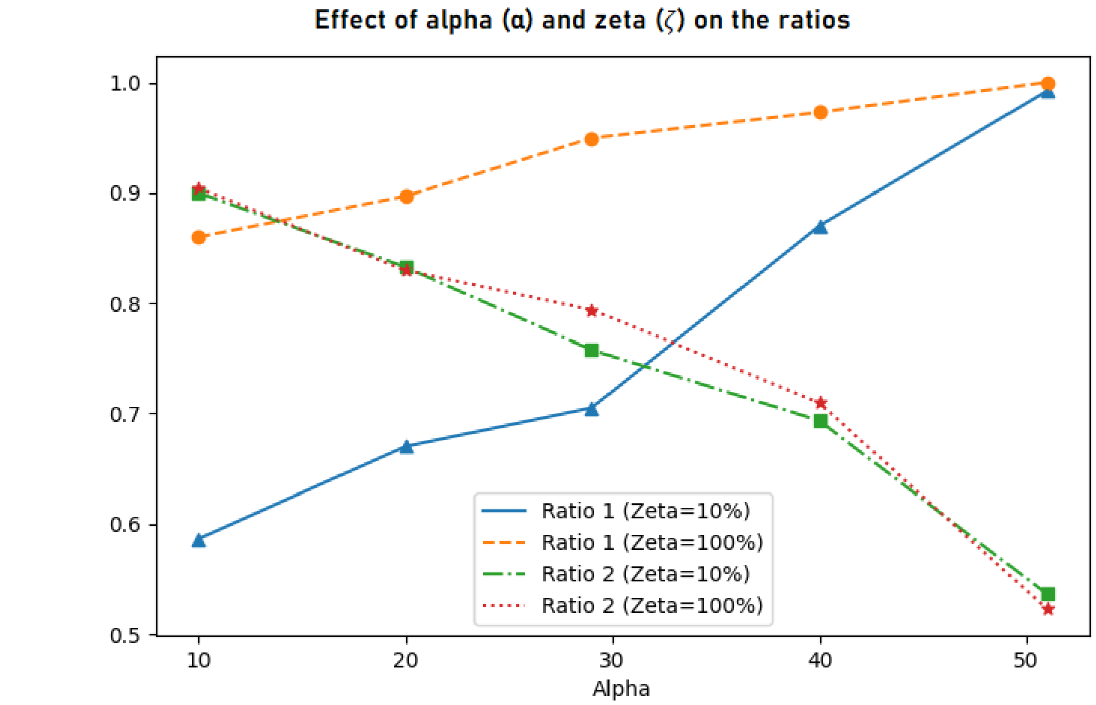
3. **Zeta (ζ) = 10%, and the adversary performs selfish mining**

The attacker is now connected to 10% of miners in the network. When the hashing power of the attacker is below 28%, the rewards of the attacker are less than when he was honest, and when the attacker's hashing power is greater than 28%, the rewards are always greater than being honest. By this, we can conclude that if the attacker has more than 28% hashing power, selfish mining makes sense, as it creates more profits than being honest.

Effect of selfish miner's hashing power (Alpha) and network connectivity (Zeta) on the ratios defined below

$$MPU_{node_{adv}} = \frac{\text{Number of block mined by an adversary in main chain}}{\text{Total number of blocks mined by an adversary}} \tag{1}$$

$$MPU_{node_{overall}} = \frac{\text{Number of block in the main chain}}{\text{Total number of blocks generated across all the nodes}} \tag{2}$$



In the above graph, the x-axis represents the hashing power of the miner, and the y-axis represents the ratio. We have plotted graphs between MPU$_{nodeadv}$ and alpha, where alpha is the hashing power of the adversary.

$\text{MPU}_{\text{nodeadv}}$ Ratio:

$\text{MPU}_{\text{nodeadv}}$ Ratio (1) is the fraction of adversary blocks in the main chain to the total blocks mined by the adversary. When the ratio is low, it means that many of the adversary's blocks are orphaned, and when the ratio is close to 1, all the adversary's blocks enter the main chain.

1. **Zeta (ζ) is low (≈10%)**
   When zeta, i.e., the connectivity of the attacker, is low, then as the hashing power of the adversary increases, the $\text{MPU}_{\text{nodeadv}}$ ratio increases. We can see when the hashing power is 10% of the total hashing power, the probability of the attacker's block getting into the final chain is 0.57, and when the attacker has more than 50% of hashing power, then the probability of the attacker's mined block getting into the final chain is close to 1.

2. **Zeta (ζ) is high (≈100%)**
   When the attacker is connected to all possible miners in the network, when the attacker sees a block mined by the honest nodes, it immediately broadcasts his own privately saved block to the network. Since the connectivity is so high, the attacker's block reaches the other miners faster than the block mined by the honest miner, and then the miners mining on the attacker's block will be more, which is actually gamma(γ), so most of the miners are mining on the attacker's block, and the attacker chain has a high probability of winning over the honest chain. The graph makes it evident that no matter the hashing power of the attacker, the $\text{MPU}_{\text{nodeadv}}$ ratio will be higher when zeta(ζ) is at 100%.

$\text{MPU}_{\text{nodeoverall}}$ Ratio:

Ratio (2) is the fraction of the main chain length to the number of blocks generated in the network. The ratio is low when there are a lot of forks, and many blocks are orphaned. Similarly, the ratio is high when there are fewer or no forks.

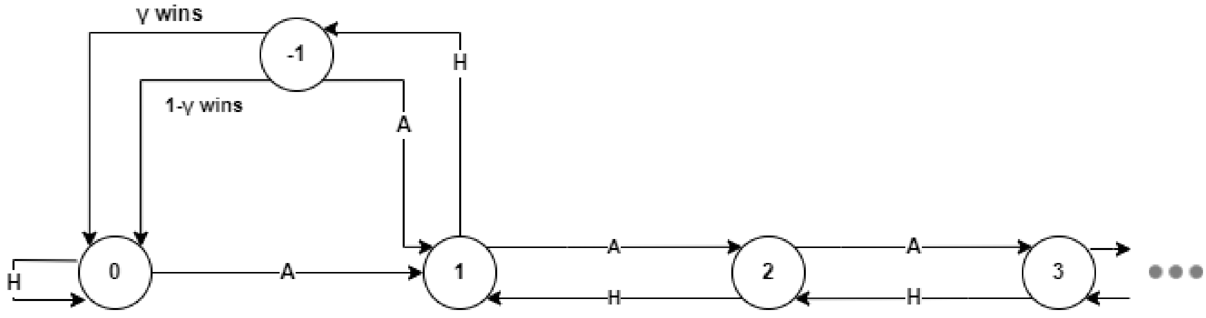
1. **Zeta (ζ) is low (≈10%) (OR) Zeta (ζ) is high (≈100%)**
   When the connectivity is 10%, we can see in the graph as the attacker's hashing power increases, the $\text{MPU}_{\text{nodeoverall}}$ ratio decreases. This is because the attacker's ability to kill the honest chain is proportional to the attacker's hashing power.

Final Insights:
ζ has no effect on the plot of ratio (2) because ζ represents the adversary's network connectivity, but the ratio is independent of who generated the block. Whether the adversary block is orphaned or an honest block is orphaned, it makes no difference; the numerator and the denominator stay the same.

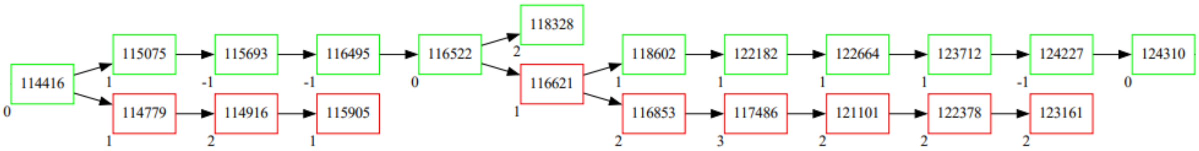
Stubborn Mining Attack and Comparison with Selfish Mining Attack

Stubborn mining attack is a variant of a selfish mining attack. The key difference between the stubborn mining strategy is that a stubborn miner does not give up when the lead goes below 2. Instead, a stubborn miner keeps mining on its private chain until the public chain becomes longer. This strategy can often increase a stubborn miner's rewards even more than a selfish-mining attacker.

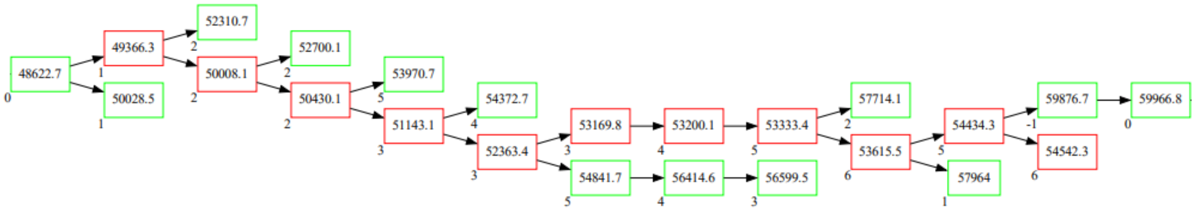
State Diagram of a Stubborn Miner



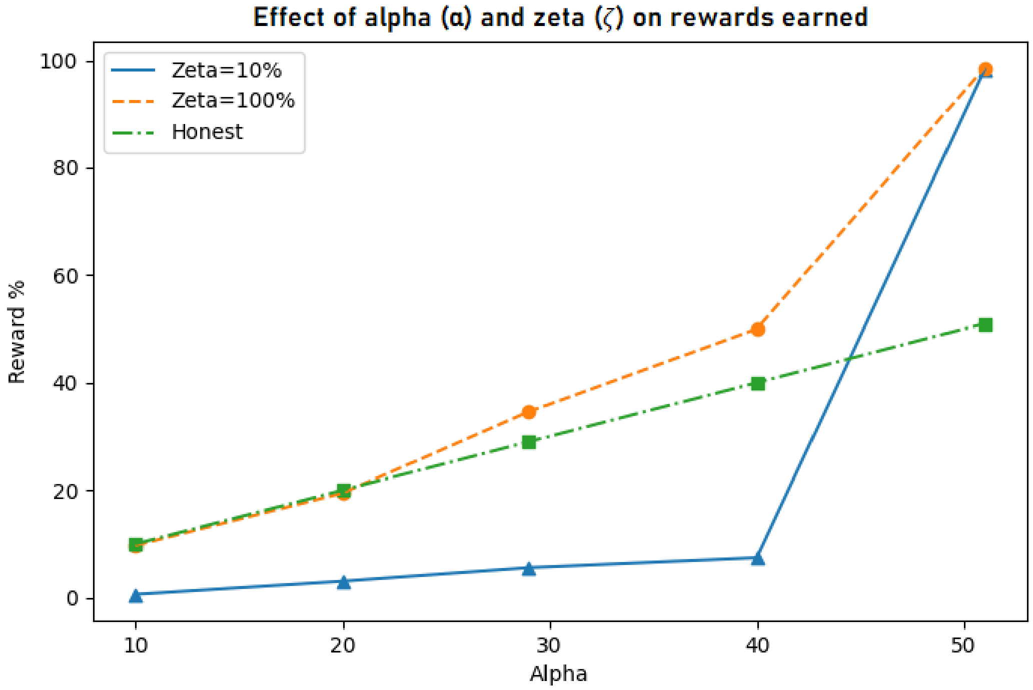
Example blockchain tree with parameters alpha = 20 and zeta = 20



Example blockchain tree with parameters alpha = 40 and zeta = 100



Effect of stubborn miner’s hashing power (Alpha) and network connectivity (Zeta) on rewards earned



In the above figure, the x-axis represents the stubborn miner’s hashing power (alpha), and the y-axis represents the rewards earned.

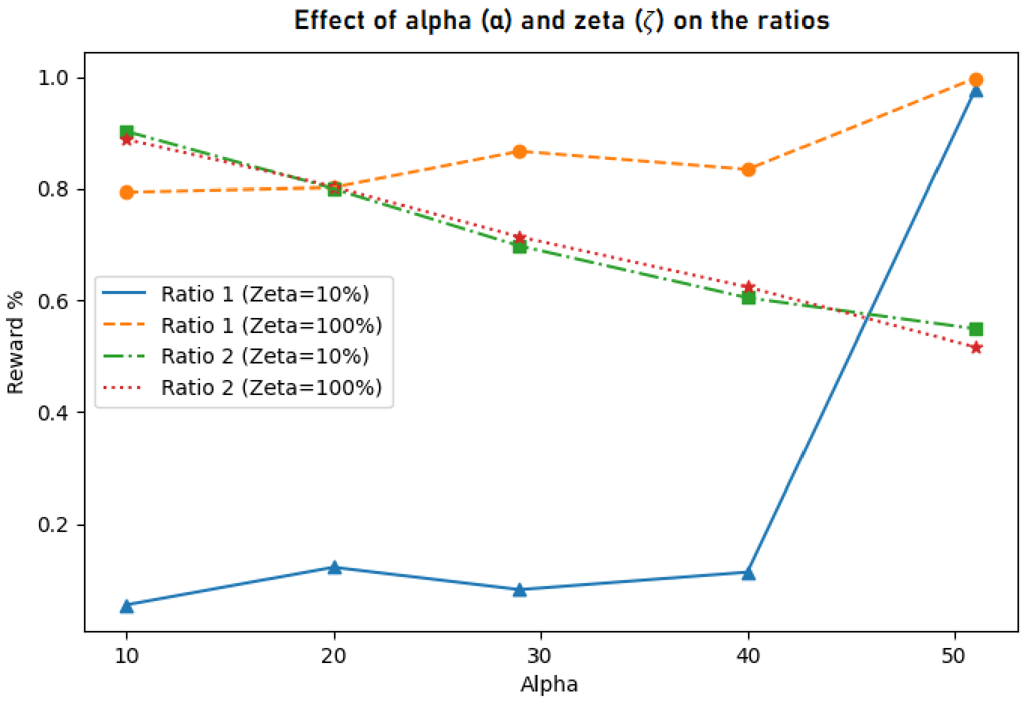
1. **Zeta (ζ) = 10%, and the adversary performs stubborn mining**
   When zeta (ζ) = 10%, the adversary is connected to only 10% of honest nodes. Thus, when the adversary makes a block public, the percentage of honest miners mining on the adversary’s block (γ) will be low. When this happens, the probability that honest miners extend the public chain ((1 - γ)(1 - α)) increases, and the adversary’s blocks will be orphaned. The stubborn miner will earn less reward than if he had been honest. In this scenario, the miner needs more than 50% of the hashing power to get rewards greater than its fraction of hashing power.

2. **Zeta (ζ) = 100%, and the adversary performs stubborn mining**
   When zeta (ζ) = 100%, the adversary is connected to all the honest nodes. Thus γ will be more than (1 - γ), and the honest miners mining on the honest block ((1 - γ)(1 - α)) will find it harder to generate a block. On the other hand, the honest miners mining on the adversary’s block (γ * (1 - α)) will easily generate a block cementing the adversary blocks in the main chain. In this scenario, the adversary will always earn more reward than its fraction of hashing power.

Effect of stubborn miner’s hashing power (Alpha) and network connectivity (Zeta) on the Ratios defined below

$$MPU_{node_{adv}} = \frac{\text{Number of block mined by an adversary in main chain}}{\text{Total number of blocks mined by an adversary}} \tag{1}$$

$$MPU_{node_{overall}} = \frac{\text{Number of block in the main chain}}{\text{Total number of blocks generated across all the nodes}} \tag{2}$$



$MPU_{nodeadv}$ Ratio:

Ratio (1) is the fraction of adversary blocks in the main chain to the total blocks mined by the adversary. When the ratio is low, it means that many of the adversary’s blocks are orphaned, and when the ratio is close to 1, all the adversary’s blocks enter the main chain.

1. **Zeta (ζ) is low (≈10%)**
   When ζ is low, γ will also be low, thus the probability that honest miners mining on the honest block ((1 - γ)(1 - α)) increases and the adversary blocks will be orphaned. This results in the ratio (1) being low. In this scenario, the ratio reaches one only when the adversary’s fraction of hashing power is more than 50%.

2. **Zeta is high (≈100%)**
   ζ being high results in γ being high. Thus the probability that an honest miner mining on an adversary's block generates a block (γ * (1 - α)) increases. The honest miners will find it difficult to orphan the adversary's block. The ratio remains relatively high for any value of α.

$\text{MPU}_{\text{nodeoverall}}$ Ratio:

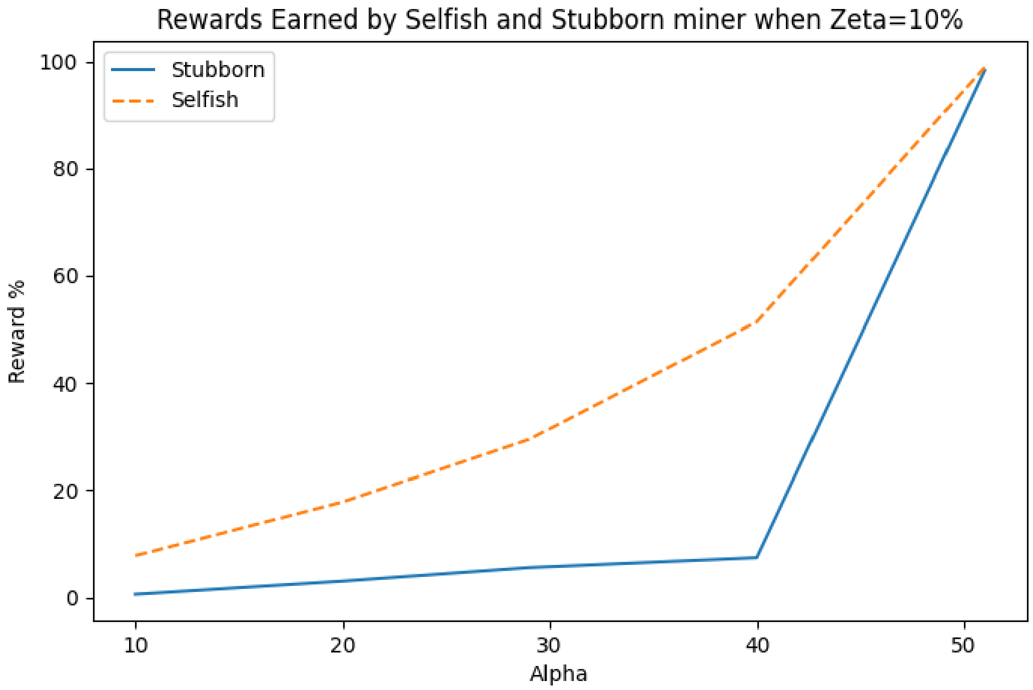
Ratio (2) is the fraction of the main chain length to the number of blocks generated in the network. The ratio is low when there are a lot of forks, and many blocks are orphaned. Similarly, the ratio is high when there are fewer or no forks.

ζ has no effect on the plot of ratio (2) because ζ represents the adversary's network connectivity, but the ratio is independent of who generated the block. Whether the adversary block is orphaned or an honest block is orphaned, it makes no difference. The numerator and the denominator stay the same.

Comparing Selfish and Stubborn Mining Attack

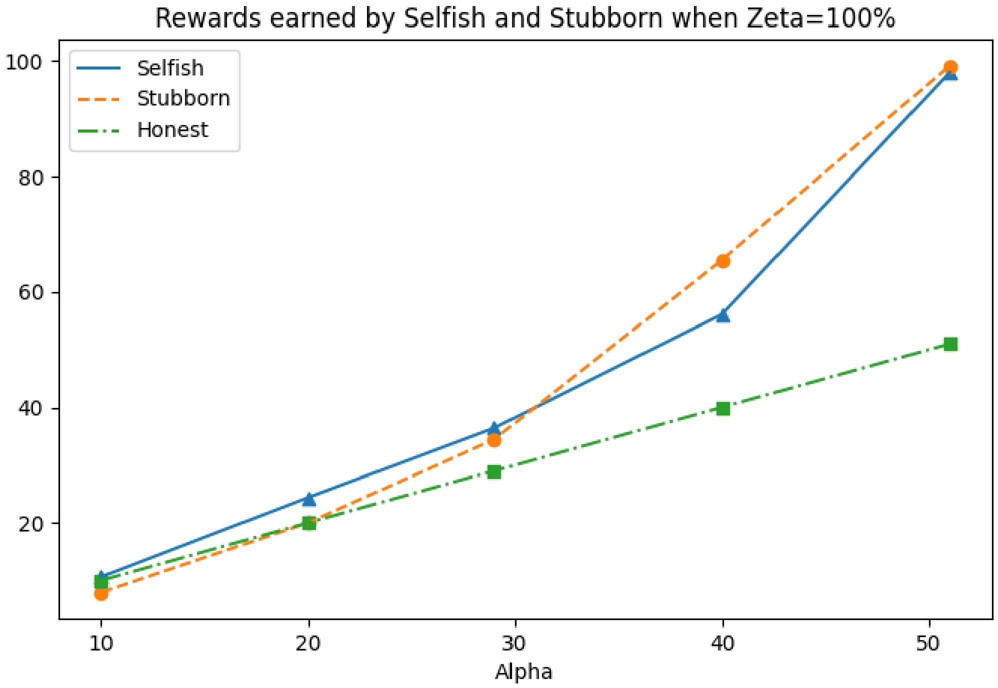
Selfish mining is not optimal for some of the parameter space, and stubborn mining gives better rewards. Some of these parameters are discussed below.

1. **Zeta (ζ) is low (≈10%)**



When ζ is low, the probability that honest miners mining on the honest block ((1 - γ)(1 - α)) increases. Stubborn miners rely on honest miners mining on adversary blocks to mine a block and cement the adversary blocks in the main chain. Because if they win, all honest nodes will start mining on this honest block or the next block released by the adversary. However, this is a risky strategy since if the ζ is low, γ will be low, and stubborn miners' blocks will be orphaned. The selfish miner plays it safe and releases the private chain once the lead goes below 0. In this scenario, when the zeta is low, selfish mining outperforms stubborn mining.

2. Zeta (ζ) is high (≈100%)



When ζ is high, stubborn mining outperforms selfish mining after a threshold alpha which in our case lies between 30% and 35% of the hashing power. Since ζ is high, (γ * (1 - α)), which is the probability that honest miner mining on an adversary's block mines a block, is also high. This means in the case of a fork, the adversary block is safe since ((1 - γ)(1 - α)) will be low, which means an honest miner will find it difficult to extend an honest chain. In this scenario, a stubborn miner can divert the majority of honest miners' hashing power. Thus overall, honest miners will generate fewer blocks than they would in selfish mining.