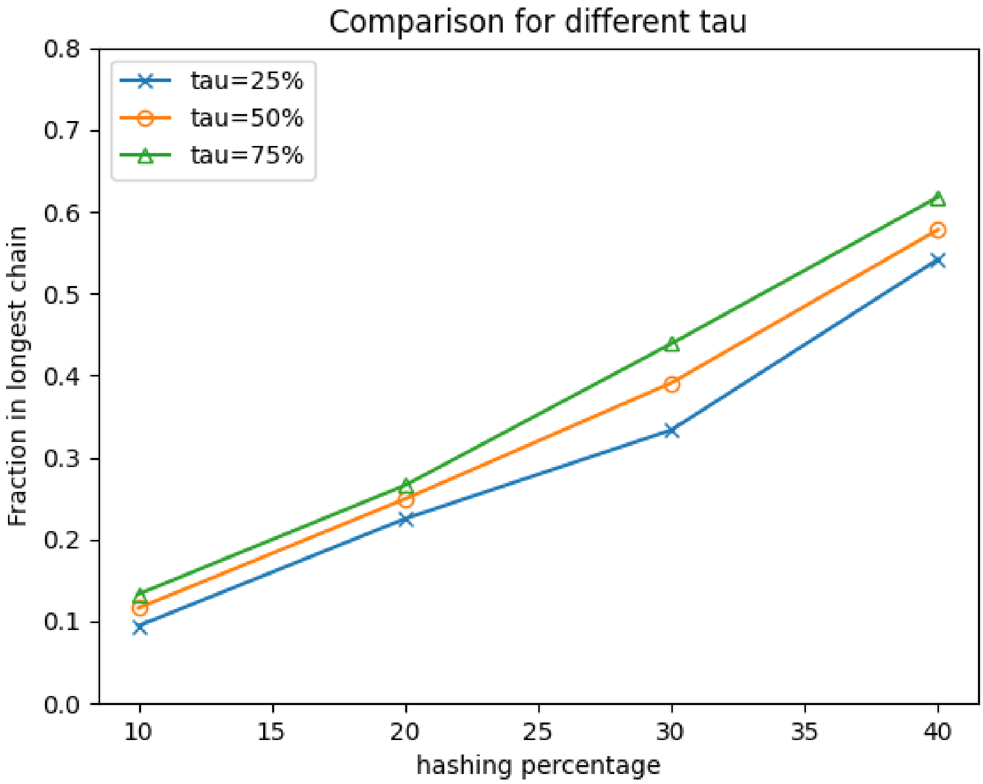
Simulating a selfish mining attack using the P2P Cryptocurrency

Advait, Ashwin, Harshvardhan
200100014, 200050016, 200050050

March 2023

1 Selfish Mining

1.1 Fraction of Adversary blocks in Main Chain



We can observe that for a given ζ as we increase the percentage of hashing power associated with the adversary, the fraction of the adversary blocks in the main chain also increases. This is because the probability of mining a block is proportional to the hashing power used for solving the associated crypto-puzzle.

Secondly, we can observe that for a given percentage of hashing power associated with the adversary, the fraction of adversary blocks in the main chain increases as we increase ζ which represents the fraction of honest nodes the adversary is connected to. This is because as we increase the fraction of honest nodes connected to the adversary, the fraction of honest nodes γ that mines on the selfish miner's block increases, and hence it increases the probability of the selfish miner's chain being included in the main chain thus increasing the fraction of adversary blocks in the main chain.

In the Eyal and Sirer paper, the theoretical result for calculating the fraction of adversary blocks in the main chain is given by

$$\mathrm{R} = \frac{\alpha(1-\alpha)^2(4\alpha+\gamma(1-2\alpha)) - \alpha^3}{1-\alpha(1+(2-\alpha)\alpha)}$$

where, α is the percentage of hashing power that the adversary has and γ is the fraction of honest nodes that are connected to the adversary.

Here we compare the values that were obtained from the simulator to the theoretical value which is calculated using the above formula.

Hashing Percentage	Experimental Value	Theoretical Value
10	0.094	0.054
20	0.2252	0.156
30	0.3335	0.3
40	0.652	0.5046

Table 1: ζ = 25%

Hashing Percentage	Experimental Value	Theoretical Value
10	0.156	0.072
20	0.219	0.1824
30	0.471	0.3268
40	0.697	0.5256

Table 2: ζ = 50%

Hashing Percentage	Experimental Value	Theoretical Value
10	0.133	0.091
20	0.2659	0.2088
30	0.4389	0.3537
40	0.6178	0.5465

Table 3: ζ = 75%

1.2 MPU Adversary

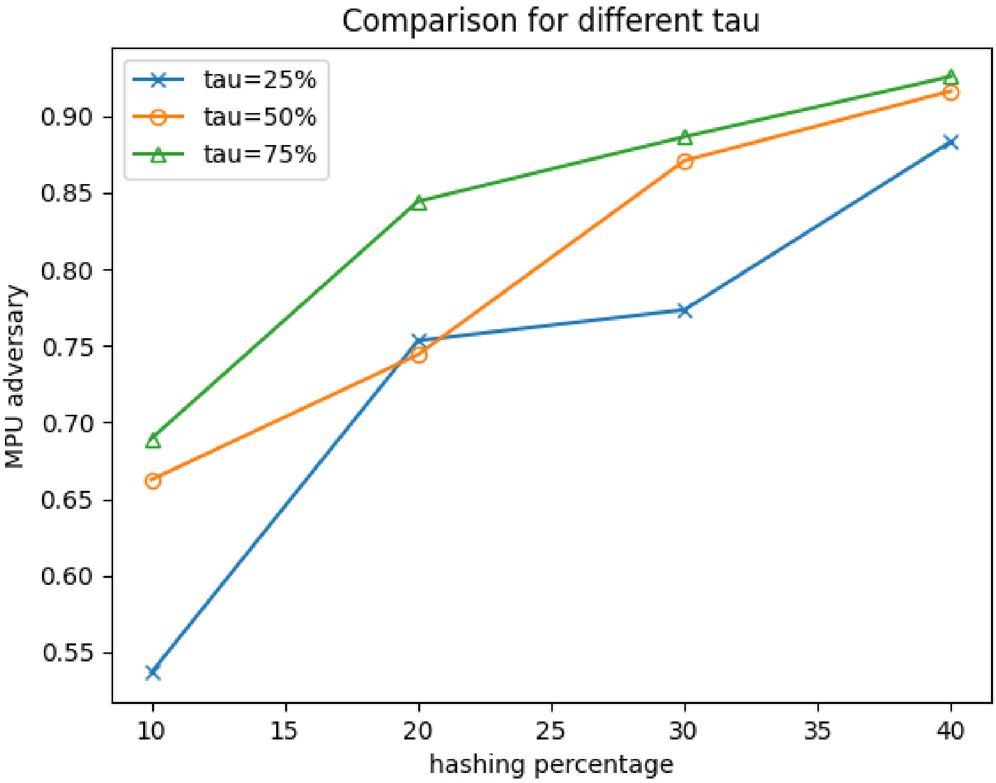
$$\mathrm{MPU}_{\mathrm{node}_{\mathrm{adv}}} = \frac{\text{Number of block mined by an adversary in main chain}}{\text{Total number of blocks mined by an adversary}}$$

We can observe that for a given ζ as we increase the percentage of hashing power associated with the adversary, the fraction of the blocks mined by the adversary that are present in the main chain also increases. This is because the probability of mining a block is proportional to the hashing power used for solving the associated crypto-puzzle.

Secondly, we can observe that for a given percentage of hashing power associated with the adversary, $\mathrm{MPU}_{\mathrm{adv}}$ increases as we increase ζ which represents the fraction of honest nodes the adversary is connected to. This is because as we increase the fraction of honest nodes connected to the adversary, the fraction of honest nodes γ that mines on the selfish miner's block increases, and hence it increases the probability of the selfish miner's chain being included in the main chain. As a result, a greater fraction of the blocks that were mined by the adversary would be included in the main chain.

	HF = 10%	HF = 20%	HF = 30%	HF = 40%
ζ = 25%	0.5367	0.7534	0.7735	0.8833
ζ = 50%	0.6625	0.7442	0.8709	0.9163
ζ = 75%	0.6894	0.8443	0.8864	0.9258

Table 4: $\mathrm{MPU}_{\mathrm{adv}}$ values for Selfish miner



1.3 MPU Overall

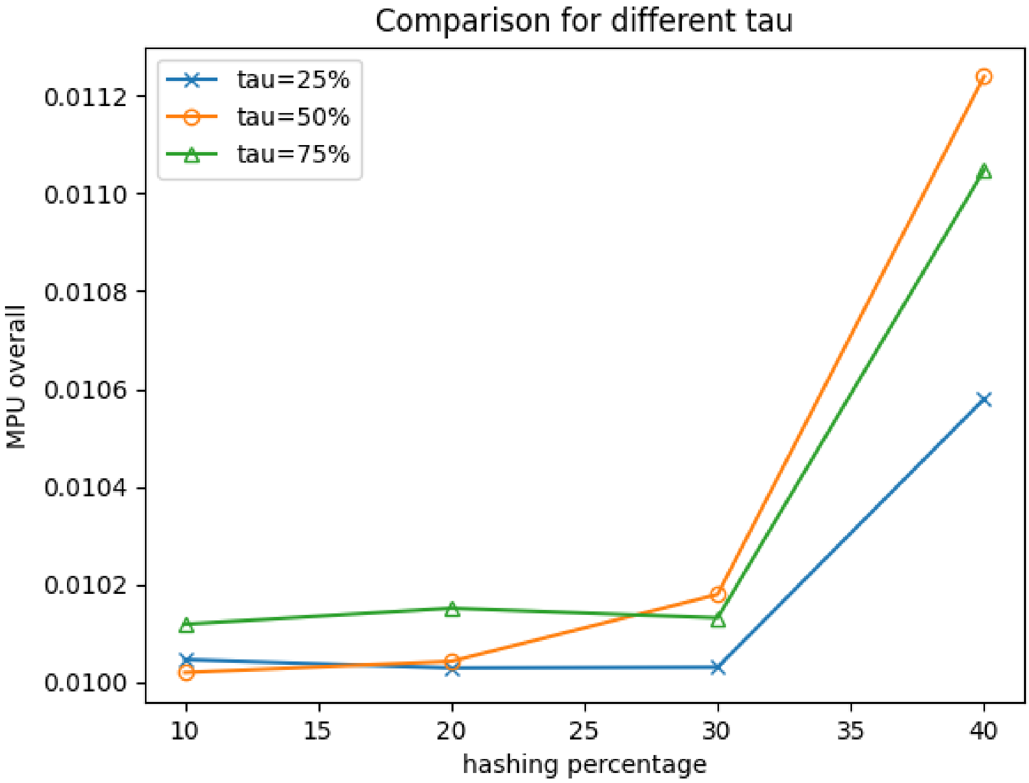
$$\mathrm{MPU}_{\mathrm{node}_{\mathrm{overall}}} = \frac{\text{Number of block in the main chain}}{\text{Total number of blocks generated across all the nodes}}$$

This quantity represents the degree of branching that has occurred in the blockchain. Due to the presence of a selfish miner, many honest miner's blocks are killed and are excluded from the main chain while the adversary blocks are included in the main chain. This results in a lot of branching in the blockchain. As it can be observed that this ratio is close to 0.01 implying that about 99% of the blocks generated by the nodes present in the network eventually are not included in the main chain.

Initially for small values of hashing percentage associated with the selfish miner, there will be more branching as most of the times the private chain of the selfish miner will be killed and won't be included in the main chain. However, for larger values of hashing percentage of the selfish miner, there will be far less branching since most of the times the selfish miner will solve the crypto-puzzle first and only his blocks will be included in the main chain.

	HF = 10%	HF = 20%	HF = 30%	HF = 40%
ζ = 25%	0.01005	0.01002	0.01003	0.01057
ζ = 50%	0.01002	0.01004	0.01017	0.01124
ζ = 75%	0.01012	0.01015	0.01013	0.01105

Table 5: $\text{MPU}_{\text{overall}}$ values for Selfish miner



2 Stubborn Mining

2.1 Fraction of Adversary blocks in Main Chain

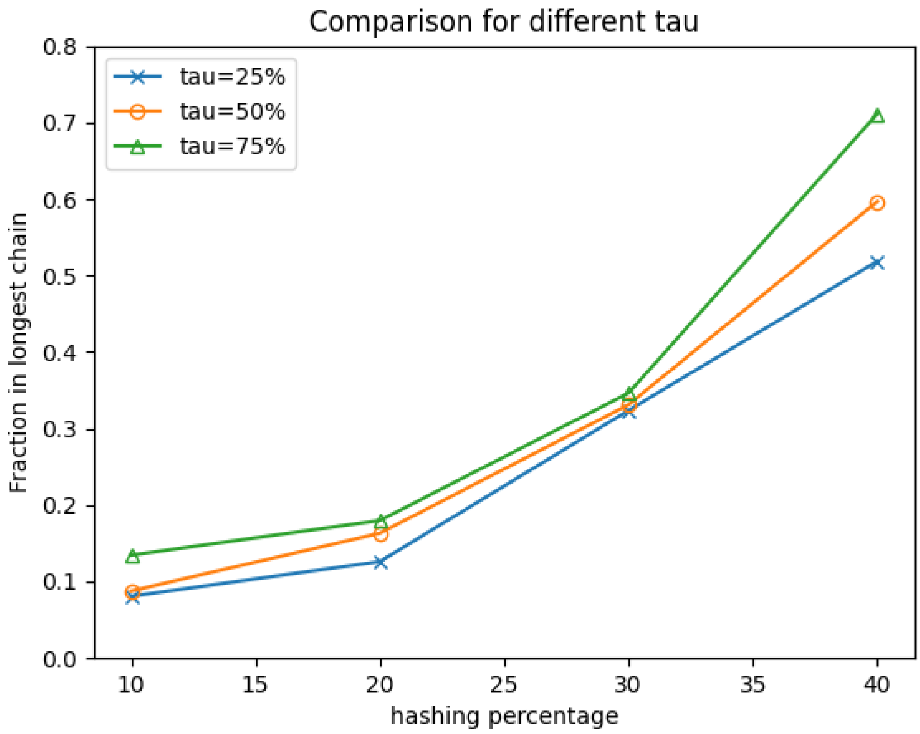
In several ways, the stubborn mining strategy follows a similar trend as the selfish mining strategy. Just as we had observed in the selfish mining strategy, for a given ζ value, the fraction of the adversary blocks in the main chain increases as we increase the percentage of hashing power associated with the adversary. The reason behind this observation is the same as in the case of selfish mining strategy which is that the probability of mining a block is proportional to the hashing power used for solving the associated crypto-puzzle.

Similarly, for a given hashing percentage associated with the adversary, the fraction of adversary blocks in the main chain increases as we increase the fraction of honest nodes the adversary is connected to. The reason behind this observation is that as we increase the fraction of honest nodes connected to the adversary, the fraction of honest nodes γ that mines on the stubborn miner's block increases, and hence it increases the probability of the stubborn miner's chain being included in the main chain thus increasing the fraction of adversary blocks in the main chain.

Finally, we can observe that for a given hashing percentage associated with the adversary and for a given value of ζ, the stubborn mining strategy outperforms the selfish mining strategy which was proved in the stubborn mining paper.

	HF = 10%	HF = 20%	HF = 30%	HF = 40%
ζ = 25%	0.0808	0.1261	0.3237	0.5187
ζ = 50%	0.0876	0.1631	0.2911	0.4967
ζ = 75%	0.1345	0.1797	0.3464	0.7113

Table 6: Fraction of Adversary blocks in Main Chain for Stubborn miner



2.2 MPU Adversary

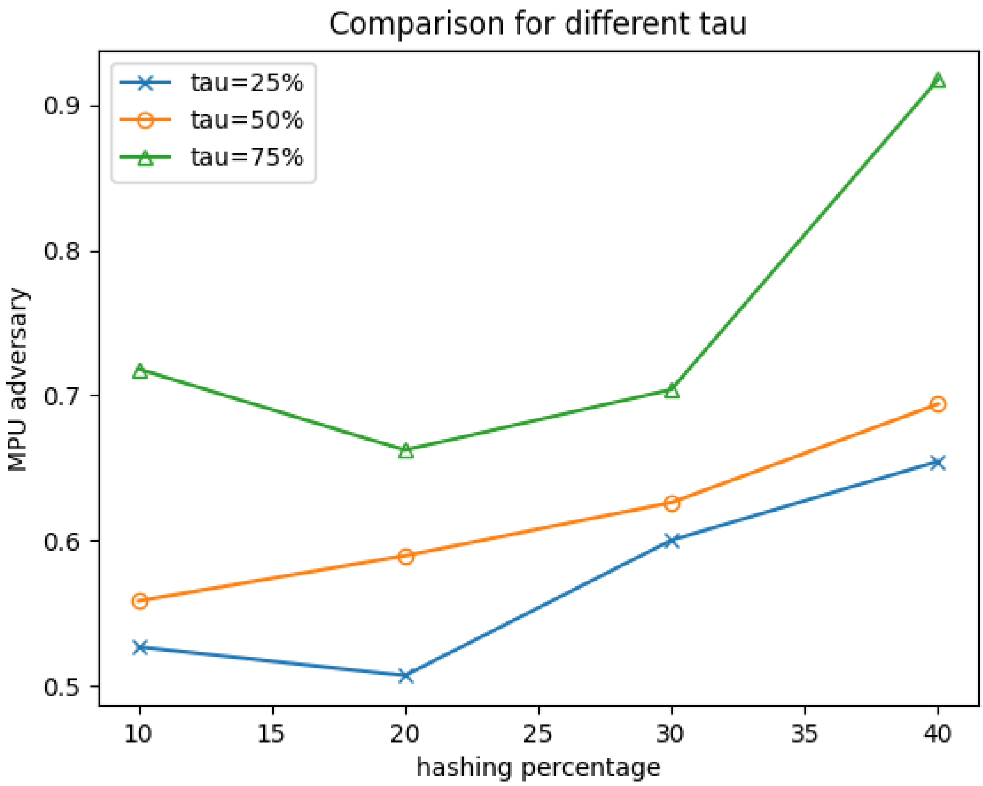
$$\text{MPU}_{\text{node}_{\text{adv}}} = \frac{\text{Number of block mined by an adversary in main chain}}{\text{Total number of blocks mined by an adversary}}$$

We can observe that for a given ζ as we increase the percentage of hashing power associated with the adversary, the fraction of the blocks mined by the adversary that are present in the main chain also increases. This is because the probability of mining a block is proportional to the hashing power used for solving the associated crypto-puzzle.

Secondly, we can observe that for a given percentage of hashing power associated with the adversary, MPU_{adv} increases as we increase ζ which represents the fraction of honest nodes the adversary is connected to. This is because as we increase the fraction of honest nodes connected to the adversary, the fraction of honest nodes γ that mines on the stubborn miner's block increases, and hence it increases the probability of the stubborn miner's chain being included in the main chain. As a result, a greater fraction of the blocks that were mined by the adversary would be included in the main chain.

	HF = 10%	HF = 20%	HF = 30%	HF = 40%
ζ = 25%	0.5267	0.5069	0.6002	0.6545
ζ = 50%	0.5583	0.5894	0.6261	0.6539
ζ = 75%	0.7181	0.6622	0.7039	0.9175

Table 7: MPU_{adv} values for Stubborn miner



2.3 MPU Overall

$$\text{MPU}_{\text{node}_{\text{overall}}} = \frac{\text{Number of block in the main chain}}{\text{Total number of blocks generated across all the nodes}}$$

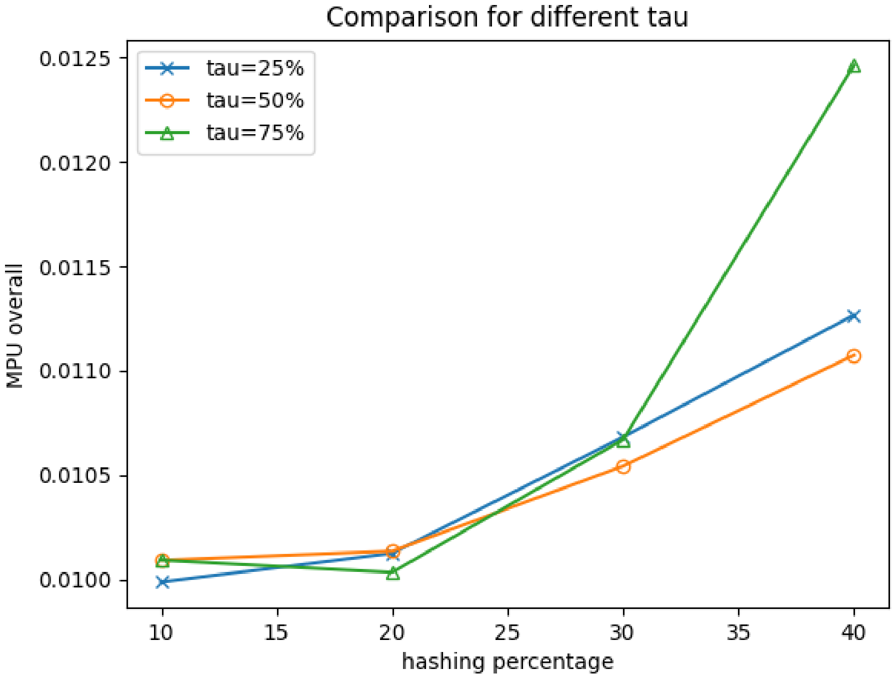
This quantity represents the degree of branching that has occurred in the blockchain. Due to the presence of a stubborn miner, many honest miner's blocks are killed and excluded from the main chain while the adversary blocks are included in the main chain. This results in a lot of branching in the blockchain. As it can be observed that this ratio is close to 0.01 implying that about 99% of the blocks generated by the nodes present in the network eventually are not included in the main chain.

Just as we had seen in the selfish mining strategy, as we increase the hashing percentage associated with the stubborn miner, there will be less branching occurring in the blockchain. As a result, this ratio increases as we increase the hashing percentage.

Moreover, this ratio for stubborn mining strategy is more than that of the selfish mining strategy. This means that there is less branching occuring in the presence of stubborn miner as compared to the presence of a selfish miner. This is because the stubborn mining strategy performs better than the selfish mining strategy and hence more stubborn miner's blocks are included in the main chain thus increasing the overall ratio.

	HF = 10%	HF = 20%	HF = 30%	HF = 40%
ζ = 25%	0.0099	0.0101	0.0107	0.0113
ζ = 50%	0.0101	0.0102	0.0105	0.0111
ζ = 75%	0.0101	0.01	0.0107	0.0124

Table 8: $\text{MPU}_{\text{overall}}$ values for Stubborn miner



3 Blockchain Trees

In this section, we have included blockchain trees formed in the simulation corresponding to different values of hashing power provided to the adversary (10%, 20%, 40%) and $\zeta = 50\%$, with rest of the parameters set as mentioned in the assignment statement. The blocks generated by adversary are colored in red.

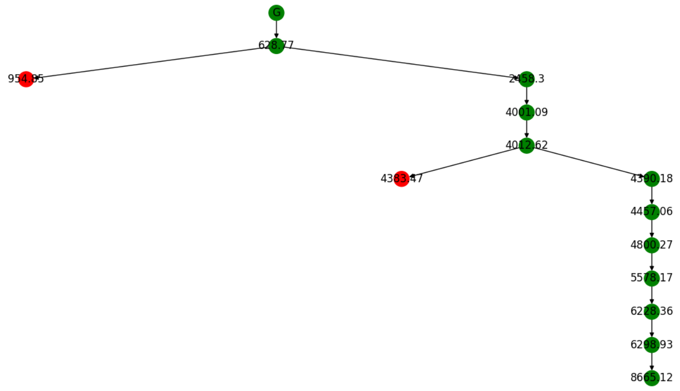


Figure 1: hashing power = 10%

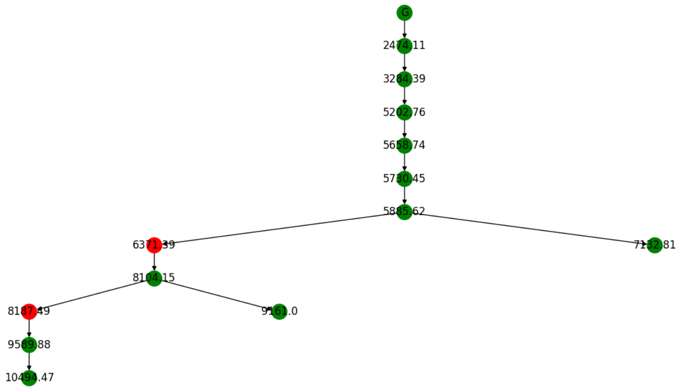


Figure 2: hashing power = 20%

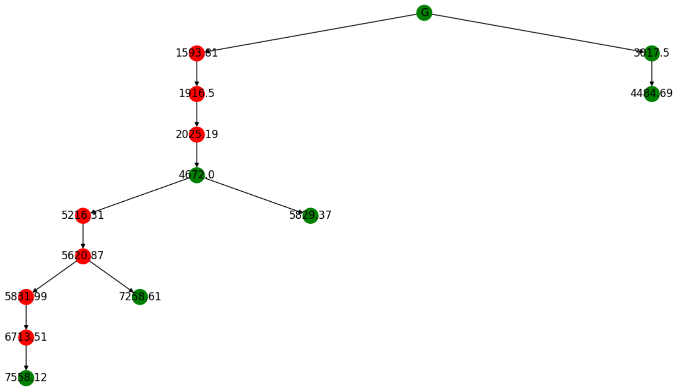


Figure 3: hashing power = 40%