CS 765 Assignment 2
Simulation of a P2P Cryptocurrency Network

Guramrit Singh 210050061

Isha Arora 210050070

Karan Godara 210050082

Indian Institute of Technology, Bombay

March 20, 2024

Contents

Visual Analysis

Note: Symbols Used in Figures and Tables

Symbol Key:

- ζ_1: Percentage of mining power of attacker-1
- ζ_2: Percentage of mining power of attacker-2
- I: Mean interarrival time between blocks
- T_{sim}: Simulation time
- ND: Not defined ($\frac{0}{0}$)

1 Effect of adversary mining powers on MPU node adversary and MPU node overall

We experimented with ζ_1 values in the range [30, 40, 50, 60, 70] and ζ_2 in the range [0, 30].

1.1 Our insight of the values for MPU node adversary

1. Keeping the value of ζ_2 fixed, as we increase the value of ζ_1, we observe that MPU node adversary of attacker 1 increases and tends to one. This is because as the hashing power of adversary 1 increases, it is able to keep up with the longest visible chain to him and maintain a lead over it. For lower values of attacker's hashing power, it is unable to launch the attack successfully many-a-times as his chain is often outpaced by the honest nodes chain and his blocks get orphaned. Hence this fraction is low for these cases. Since lead is maintained with each increasing value of ζ_1, he never faces situations where his blocks might be dropped or not accepted due to entering in the competition with the honest nodes or the other adversary. This effect is seen quantitatively in the following diagrams where we observe how when ζ_2 is fixed at 0, the value of MPU node adversary becomes 0.788, 0.917, 0.978, 1.0 and 1.0 for the ζ_1 30, 40, 50, 60 and 70 respectively. Likewise, when ζ_2 is fixed at 30, the value of MPU node adversary becomes 0.852, 1.0, 1.0 and 1.0 for the ζ_1 30, 40, 50 and 60.

2. The value of MPU node adversary of attacker 1 reaches approximately 1 when its hashing power becomes more than honest node because it mostly is able to outpace the honest miner chain. As soon as honest nodes release a block, attacker being in lead is able to release a block from its private chain and hence making sure his chain is the longest chain.

3. Note, the value of MPU node adversary of attacker 1 reaches 1 faster when ζ_2 is 30 compared to when it is 0 because to outpace honest nodes, attacker needs more hashing power than honest nodes, which becomes possible when it has more than 50 percent hashing power in case when ζ_2 is 0, whereas when ζ_2 is 30, attacker 1 only needs to have more than 35 percent hashing power. Note, here attacker 1 need not outpace attacker 2 as such, cause if attacker 2 is having higher fraction, it doesn't compete with attacker 1 directly rather it keeps adding to its private chain, its only when honest nodes release a block, attacker 1 is forced to release blocks to make sure his chain becomes accepted as longest chain in blockchain.

4. We also observe that with increasing hashing fraction ζ_1 of attacker 1. The MPU node adversary 2 decreases and tends to 0 because adversary 1 is also able to outpace attacker 2 similar to honest nodes. Hence the private chain on which atatcker 2 is working on isn't usually incorporated into longest visible block chain and hence its effort goes to vain more often.

5. As the neighbors of each node are limited between 3 and 6. With increasing the number of nodes in a graph, the topology of the network created plays a crucial role in determining the above fractions especially since we are running simulation only for a limited time. In some cases, what happens is that based on the network topology that gets selected, the blocks reaching attacker post its release by the honest miner had already reached many other honest nodes who correspondingly update their longest chain. Hence even though the attacker might have many private blocks, its chain-equalising block reaches other nodes later than the one generated by the honest node. Hence if we simulate for fixed time, we may see that sometimes the MPU node adversary seems very low and that happens due to the reasons mentioned above. Had we run it for more time, eventually (cause of low probability) honest people would accept adversaries chain as the longest but it would take some time.

1.2 Our insight of the values for MPU node overall

1. With the increasing total value of hashing fractions of attacker we observe that MPU node overall decreases and saturates at a lower bound determined by the values of ζ_1 and ζ_2 values as described ahead. This observation can be observed qualitatively, MPU node overall has value 0.707, 0.667, 0.571, 0.494 and 0.508 when ζ_1, ζ_2 has values (30,0), (40,0), (50,0), (60,0) and (70,0) respectively. Likewise, MPU node overall has value 0.494, 0.379, 0.368 and 0.359 when ζ_1, ζ_2 has values (30,30), (40,30), (50,30) and (60,30) respectively.

2. The value of MPU node overall decreases as value of attackers' hashing power increases, because with increasing values of attackers' hashing power, more and more blocks released by honest nodes get orphaned because longest chain becomes the one made by attackers. Note the orphaned blocks of the attacker with a lower hashing fraction than the other attacker also contribute to the decrease of MPU node overall as explained above.

3. Observe in above stated values, that when both ζ_1 and ζ_2 are non-zero and becomes greater than hashing power of honest nodes the value of MPU node overall saturates close to 0.33 whereas when one of the adversary has 0 hashing power (in our case ζ_2), the value of MPU node overall saturates close to 0.5. Note this happens, cause when attackers have hashing fraction more than honest node, they are mostly able to maintain lead with honest nodes and they release blocks only to equalise the length of longest chain made by honest nodes. So each attacker contributes one chain of equal length in the blockchain. Hence, when both attacker are active, the value of MPU node overall reaches $\frac{1}{3}$, whereas when only one of them is active, the value of MPU node overall reaches $\frac{1}{2}$.

Category	**MPU node value**
Attacker 1	0.6964285714285714
Attacker 2	ND
Overall	0.7357512953367875

Table 1: MPU node statistics for parameters: $\zeta_1 = 30$, $\zeta_2 = 0$, $I = 5$ s, $T_{sim} = 1000$ s

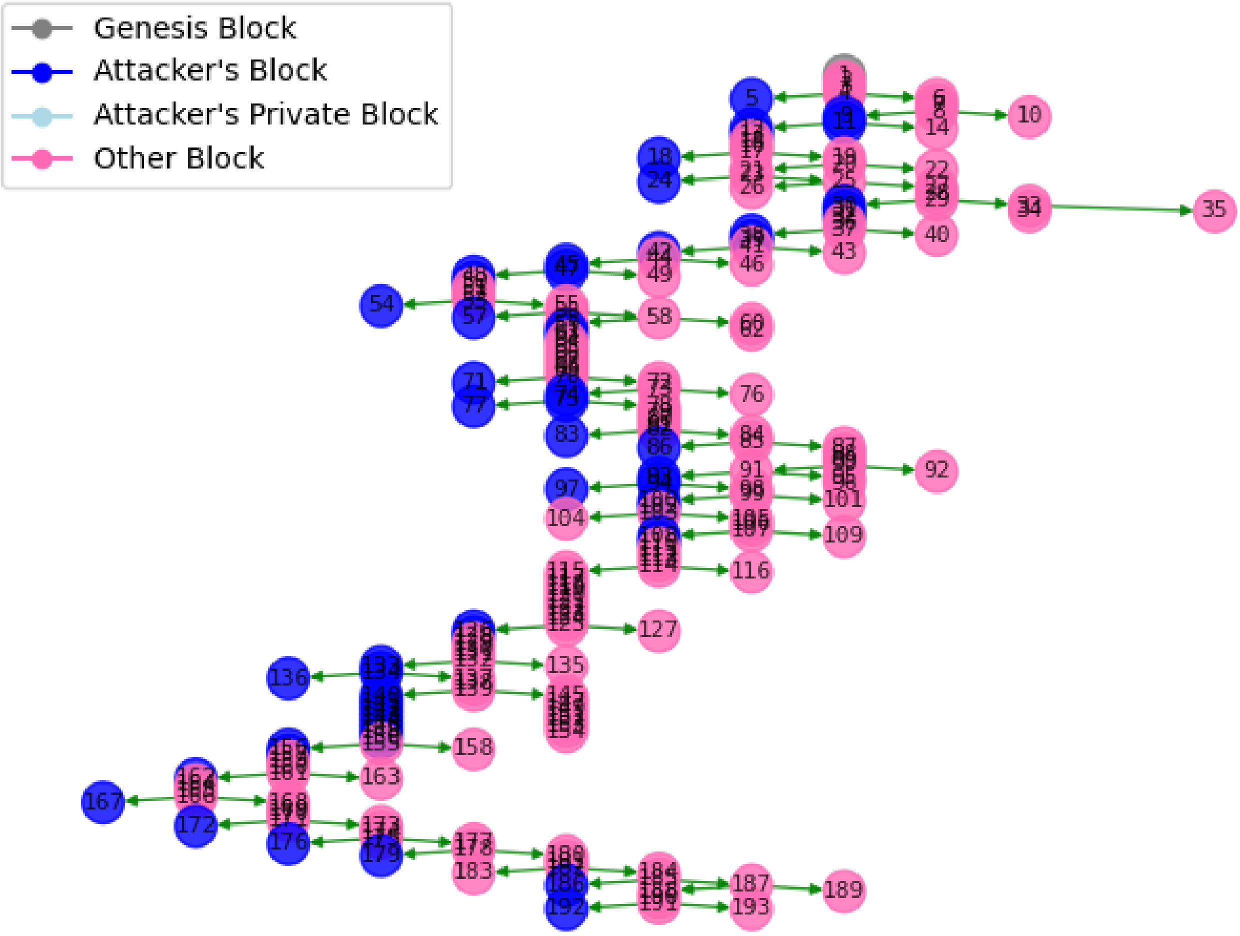

Figure 1: [Attacker-1's view] Parameters: $\zeta_1 = 30$, $\zeta_2 = 0$, $I = 5$ s, $T_{sim} = 1000$ s

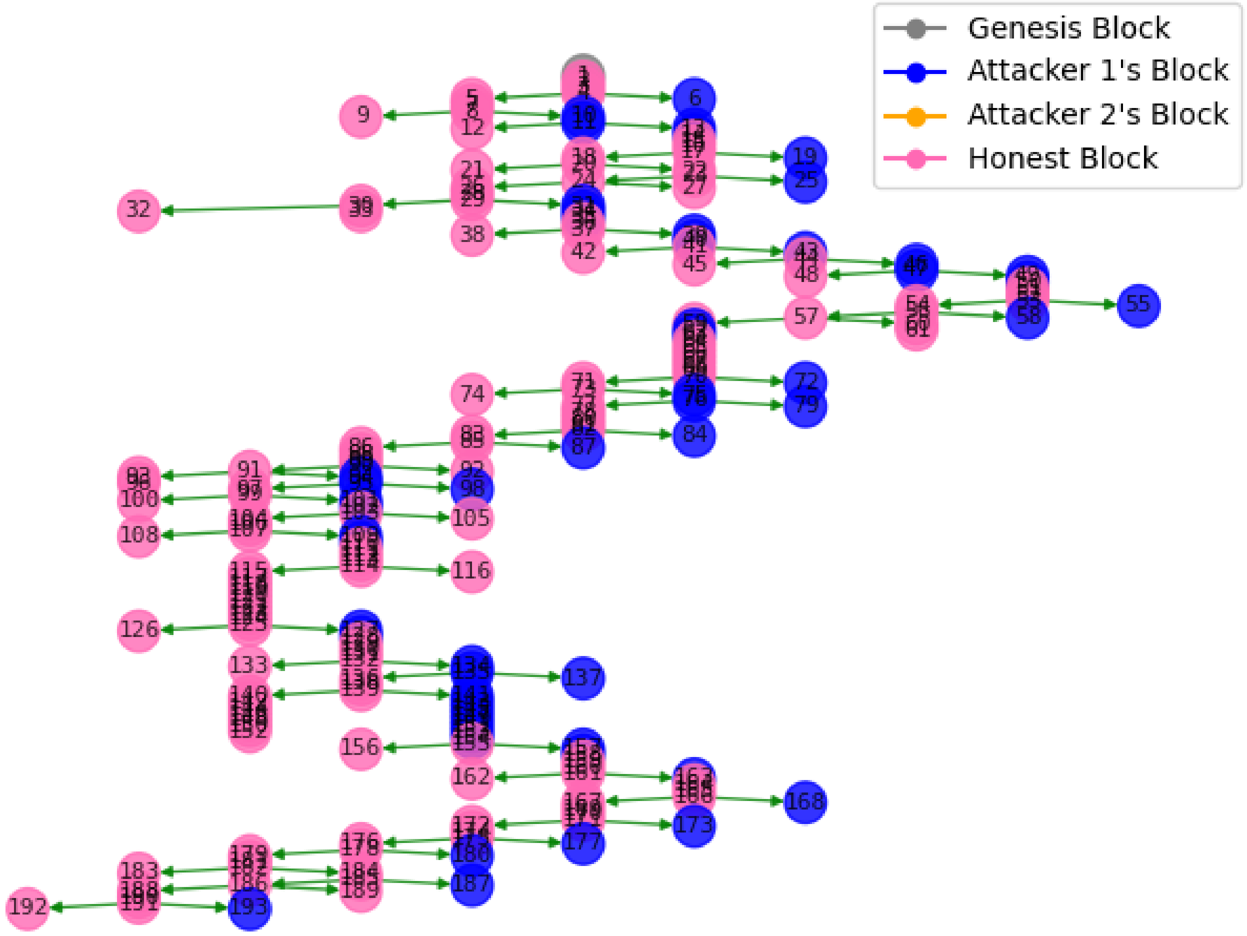

Figure 2: [Honest miner's view] Parameters: $\zeta_1 = 30$, $\zeta_2 = 0$, $I = 5$ s, $T_{sim} = 1000$ s

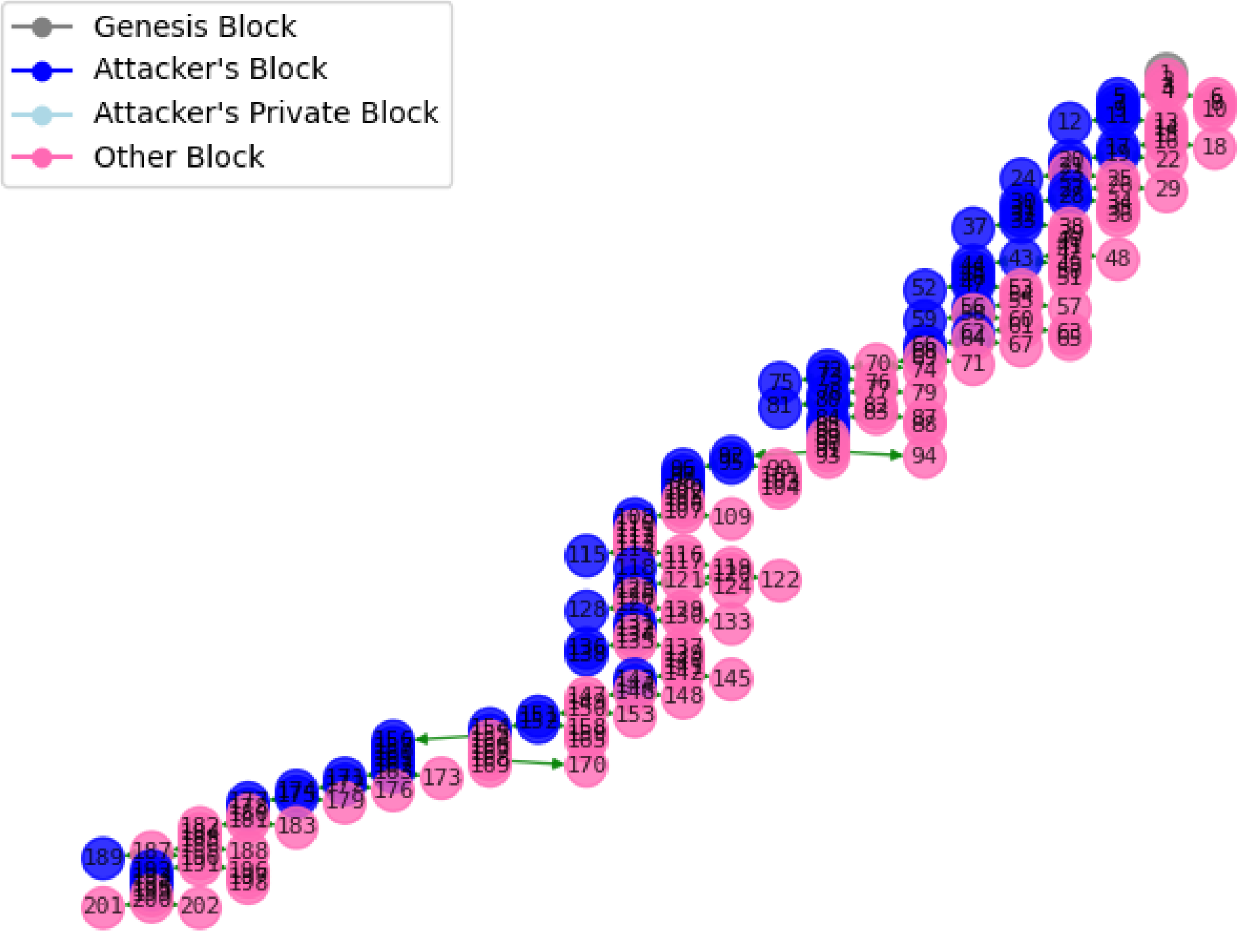

Figure 3: [Attacker-1's view] Parameters: $\zeta_1 = 40$, $\zeta_2 = 0$, $I = 5$ s, $T_{sim} = 1000$ s

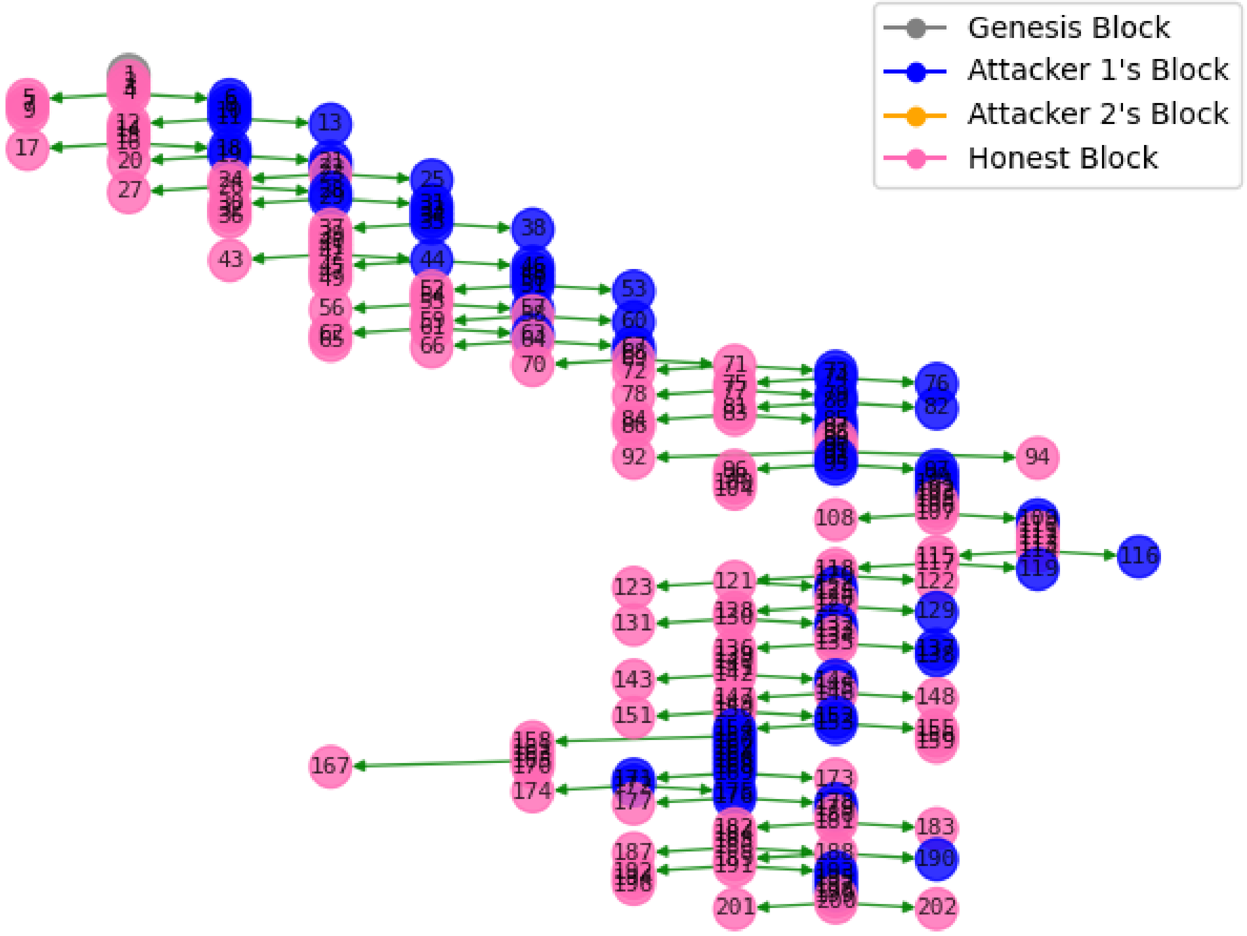

Figure 4: [Honest miner's view] Parameters: $\zeta_1 = 40$, $\zeta_2 = 0$, $I = 5$ s, $T_{sim} = 1000$ s

Category	MPU node value
Attacker 1	0.8333333333333334
Attacker 2	ND
Overall	0.6732673267326733

Table 2: MPU node statistics for parameters: $\zeta_1 = 40$, $\zeta_2 = 0$, $I = 5$ s, $T_{sim} = 1000$ s

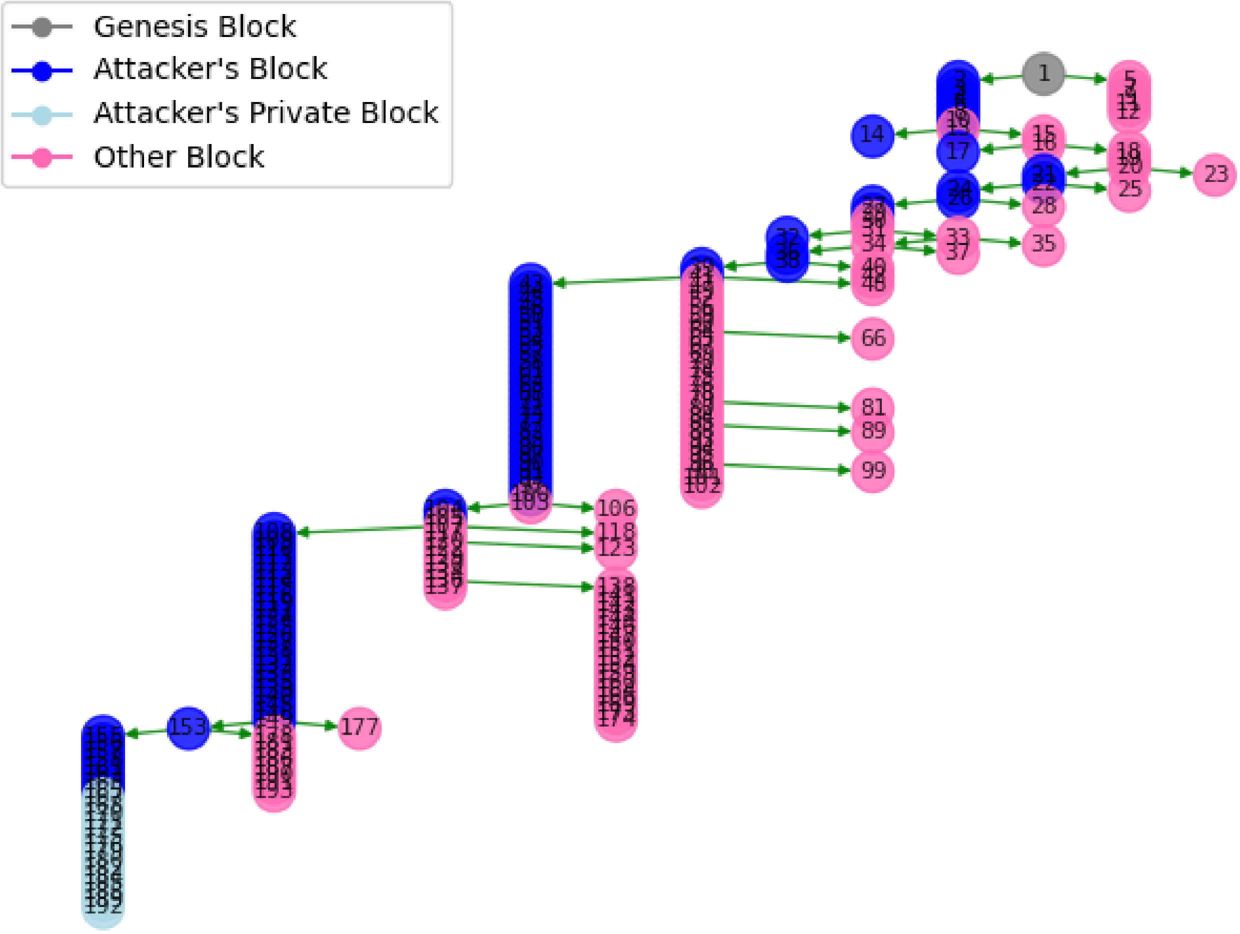

Figure 5: [Attacker-1's view] Parameters: $\zeta_1 = 50$, $\zeta_2 = 0$, $I = 5$ s, $T_{sim} = 1000$ s

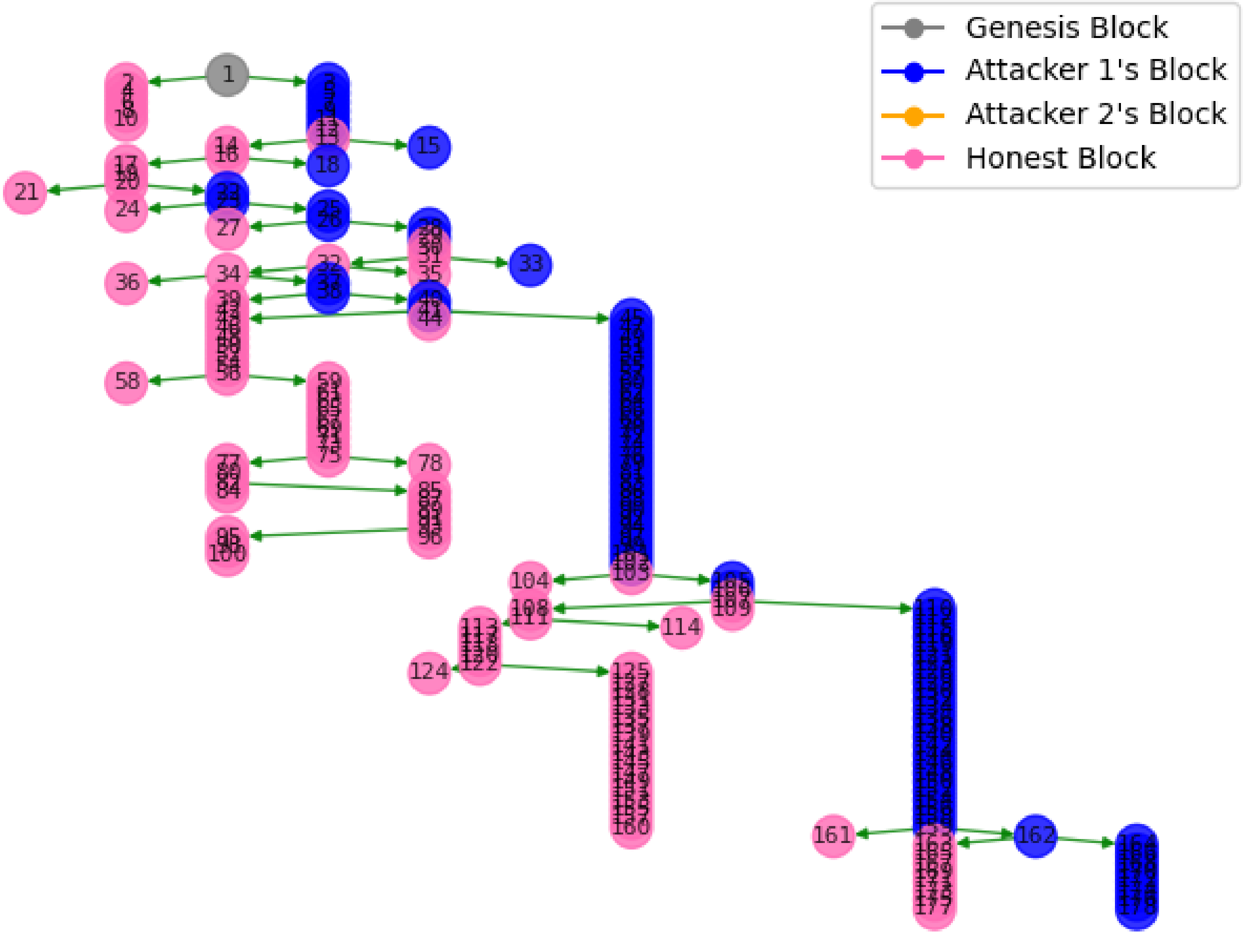

Figure 6: [Honest miner's view] Parameters: $\zeta_1 = 50$, $\zeta_2 = 0$, $I = 5$ s, $T_{sim} = 1000$ s

Category	MPU node value
Attacker 1	0.8674698795180723
Attacker 2	ND
Overall	0.5224719101123596

Table 3: MPU node statistics for parameters: $\zeta_1 = 50$, $\zeta_2 = 0$, $I = 5$ s, $T_{sim} = 1000$ s

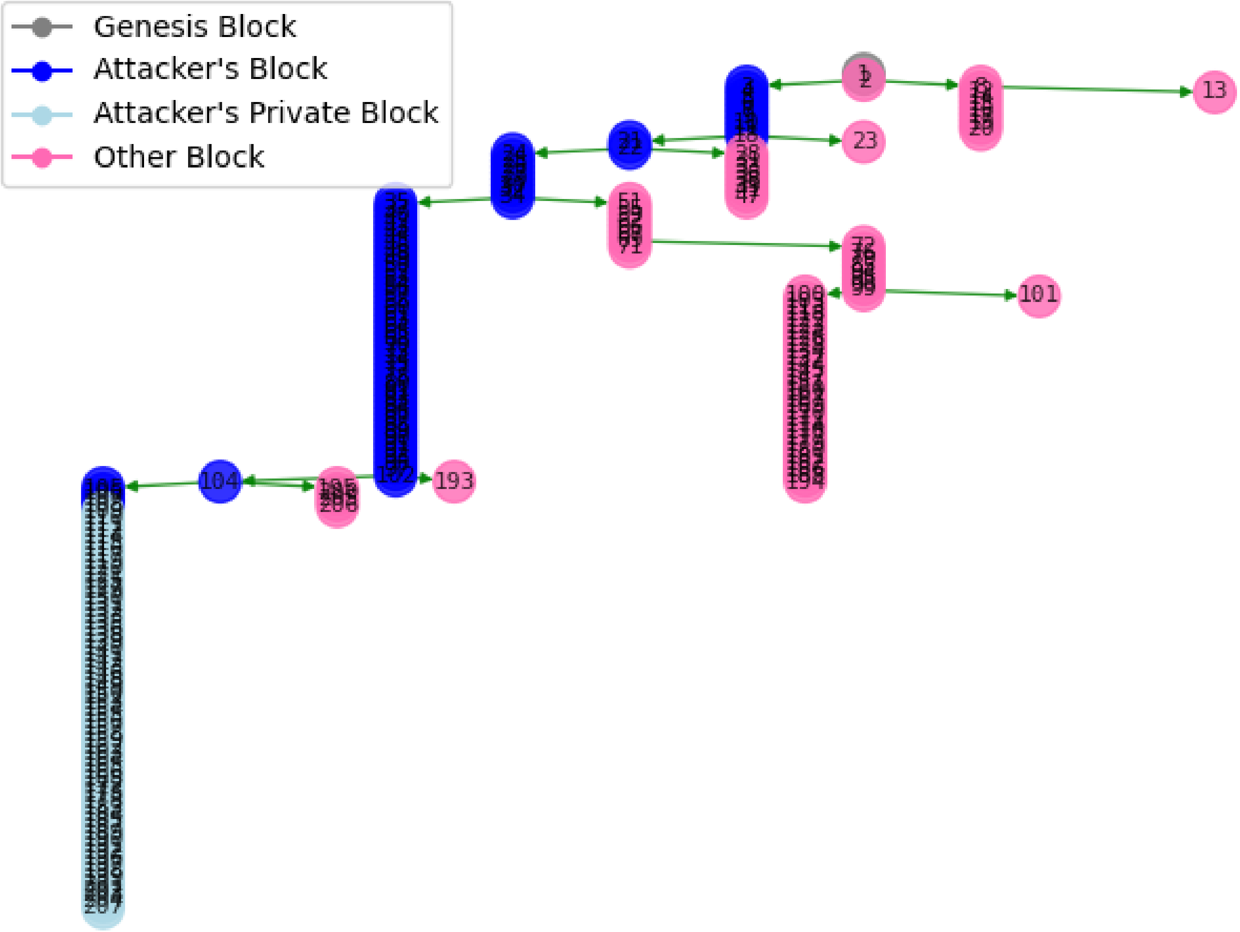

Figure 7: [Attacker-1's view] Parameters: $\zeta_1 = 60$, $\zeta_2 = 0$, $I = 5$ s, $T_{sim} = 1000$ s

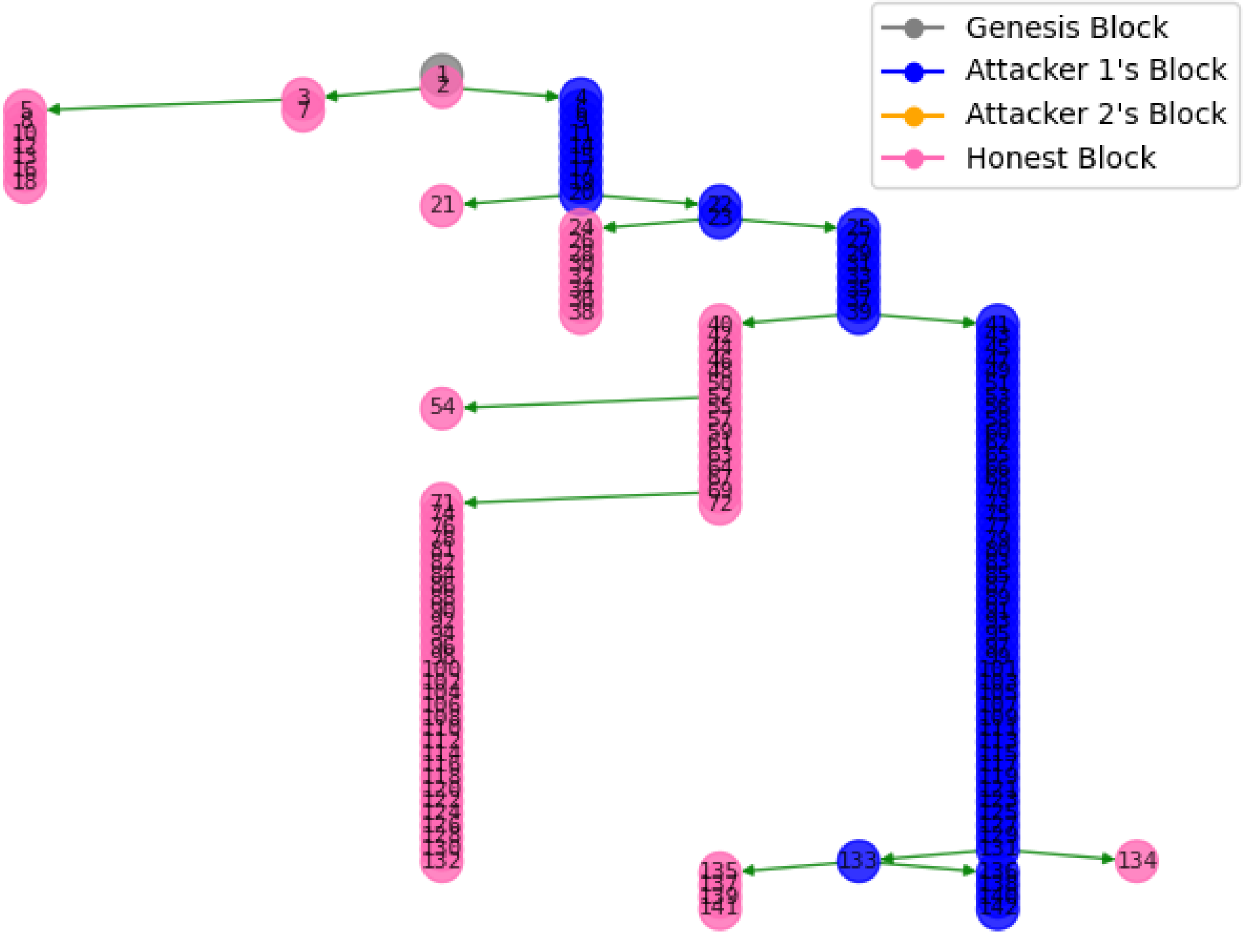

Figure 8: [Honest miner's view] Parameters: $\zeta_1 = 60$, $\zeta_2 = 0$, $I = 5$ s, $T_{sim} = 1000$ s

Category	**MPU node value**
Attacker 1	0.9420289855072463
Attacker 2	ND
Overall	0.5

Table 4: MPU node statistics for parameters: $\zeta_1 = 60$, $\zeta_2 = 0$, $I = 5$ s, $T_{sim} = 1000$ s

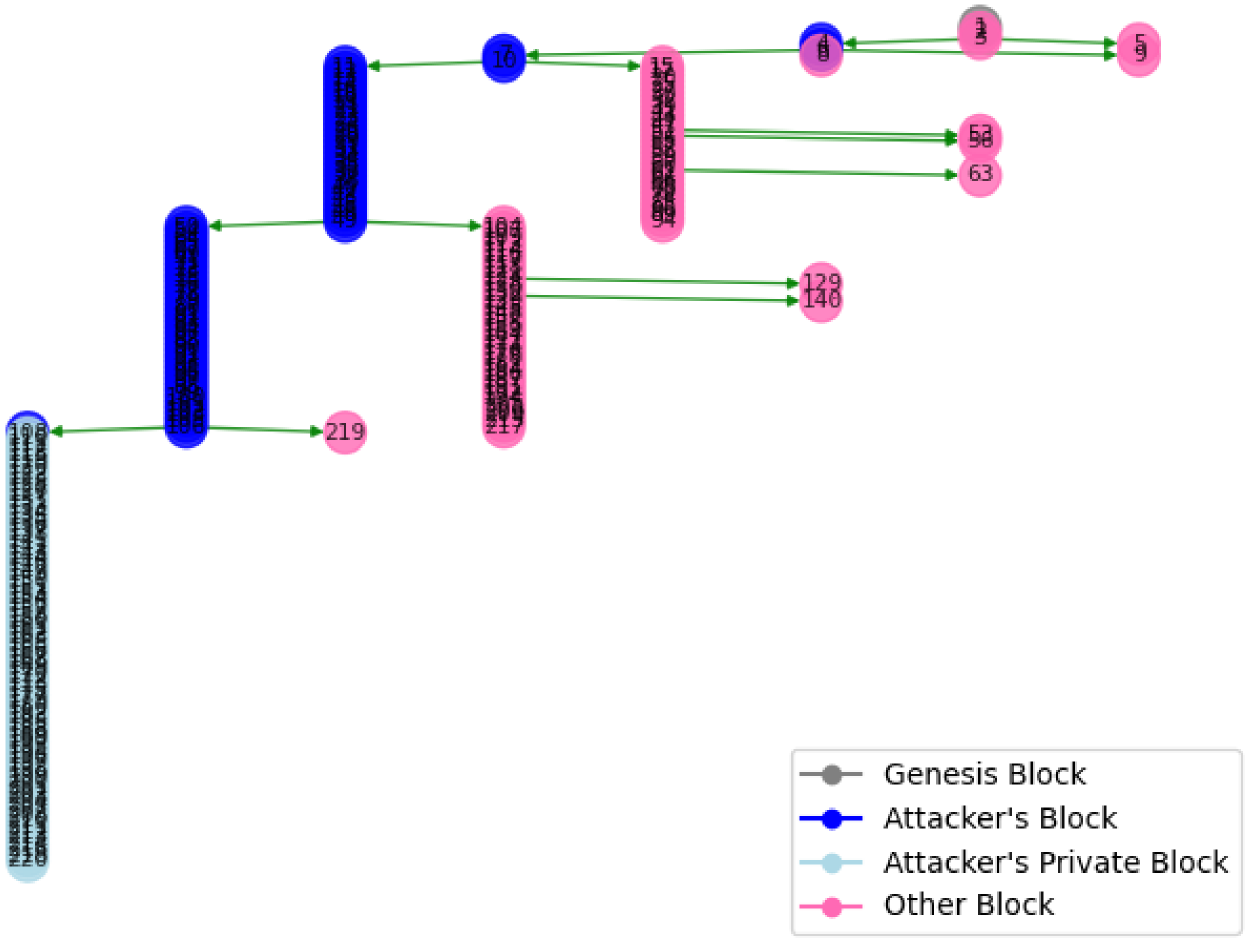

Figure 9: [Attacker-1's view] Parameters: $\zeta_1 = 70$, $\zeta_2 = 0$, $I = 5$ s, $T_{sim} = 1000$ s

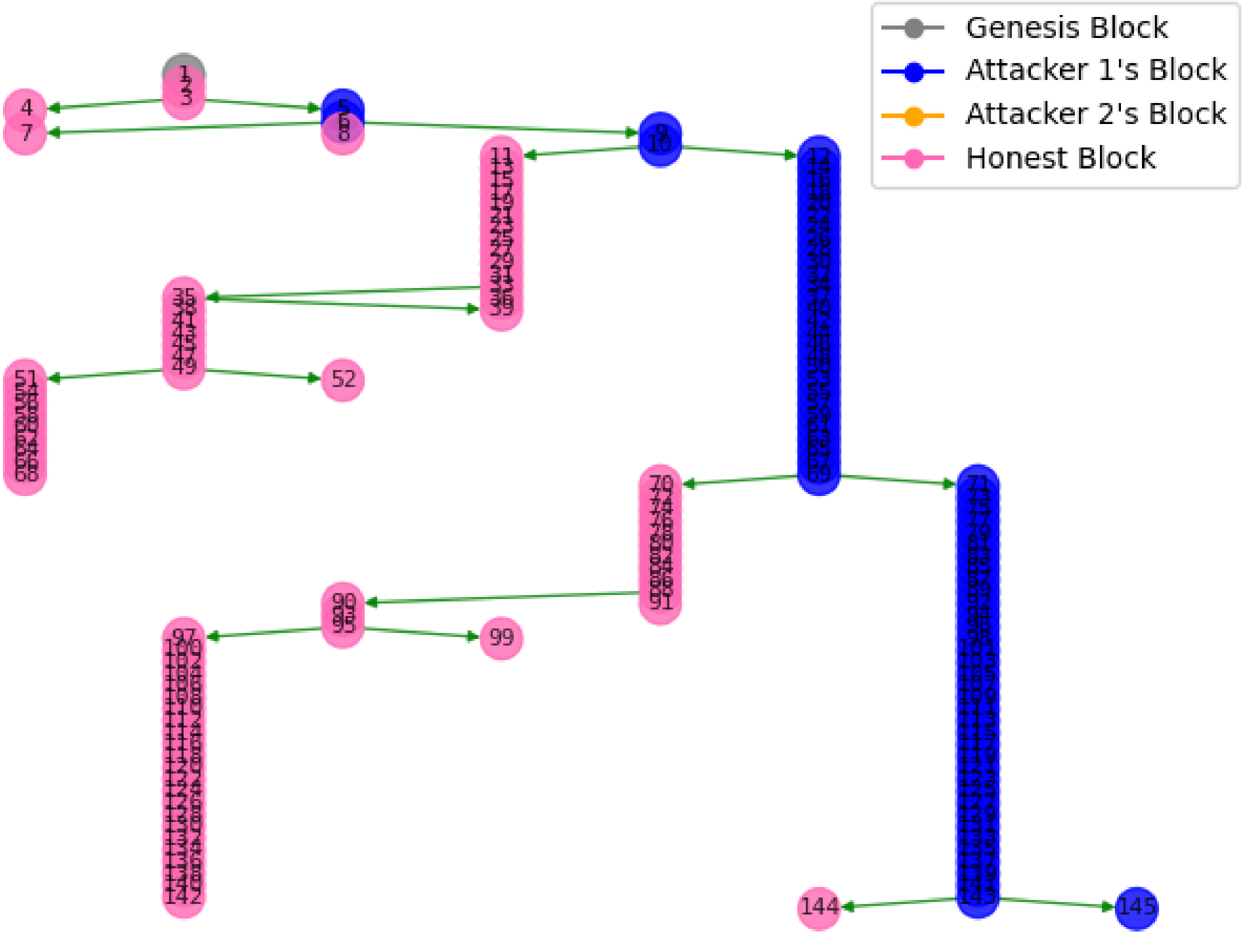

Figure 10: [Honest miner's view] Parameters: $\zeta_1 = 70$, $\zeta_2 = 0$, $I = 5$ s, $T_{sim} = 1000$ s

Category	MPU node value
Attacker 1	0.9855072463768116
Attacker 2	ND
Overall	0.496551724137931

Table 5: MPU node statistics for parameters: $\zeta_1 = 70$, $\zeta_2 = 0$, $I = 5$ s, $T_{sim} = 1000$ s

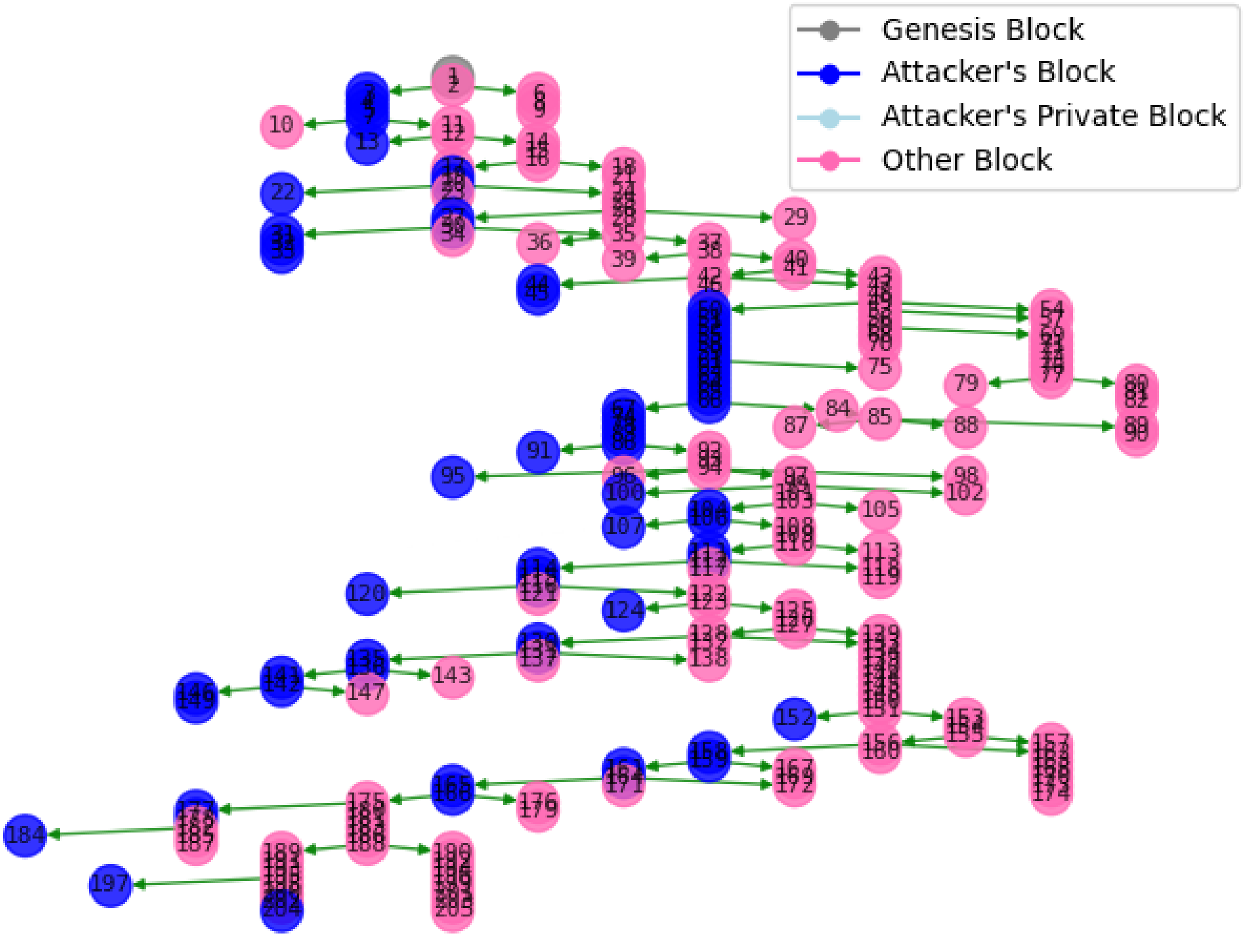

Figure 11: [Attacker-1's view] Parameters: $\zeta_1 = 30$, $\zeta_2 = 30$, $I = 5$ s, $T_{sim} = 1000$ s

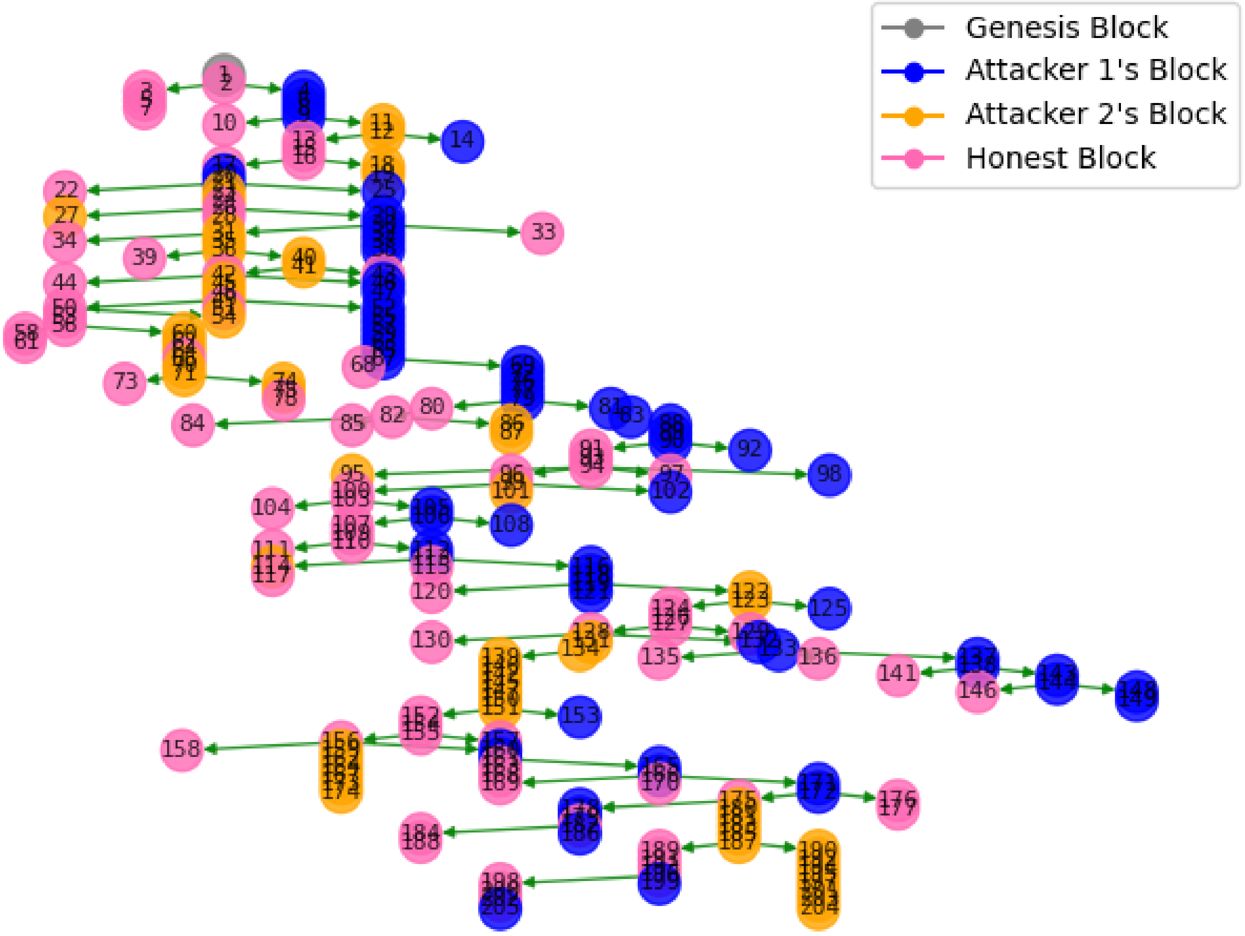

Figure 12: [Honest miner's view] Parameters: $\zeta_1 = 30$, $\zeta_2 = 30$, $I = 5$ s, $T_{sim} = 1000$ s

Category	MPU node value
Attacker 1	0.6
Attacker 2	0.4827586206896552
Overall	0.4926829268292683

Table 6: MPU node statistics for parameters: $\zeta_1 = 30$, $\zeta_2 = 30$, $I = 5$ s, $T_{sim} = 1000$ s

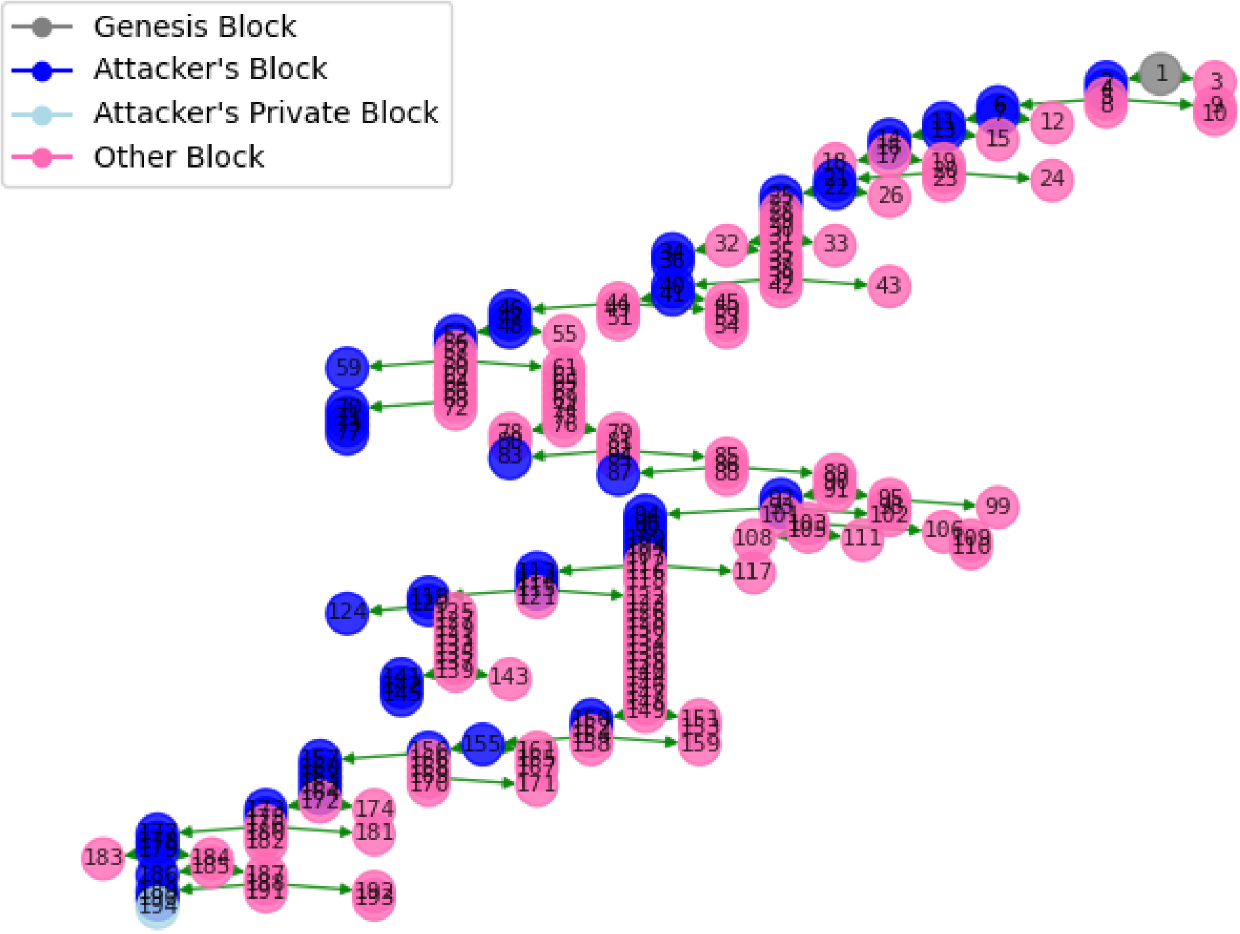

Figure 13: [Attacker-1's view] Parameters: $\zeta_1 = 40$, $\zeta_2 = 30$, $I = 5$ s, $T_{sim} = 1000$ s

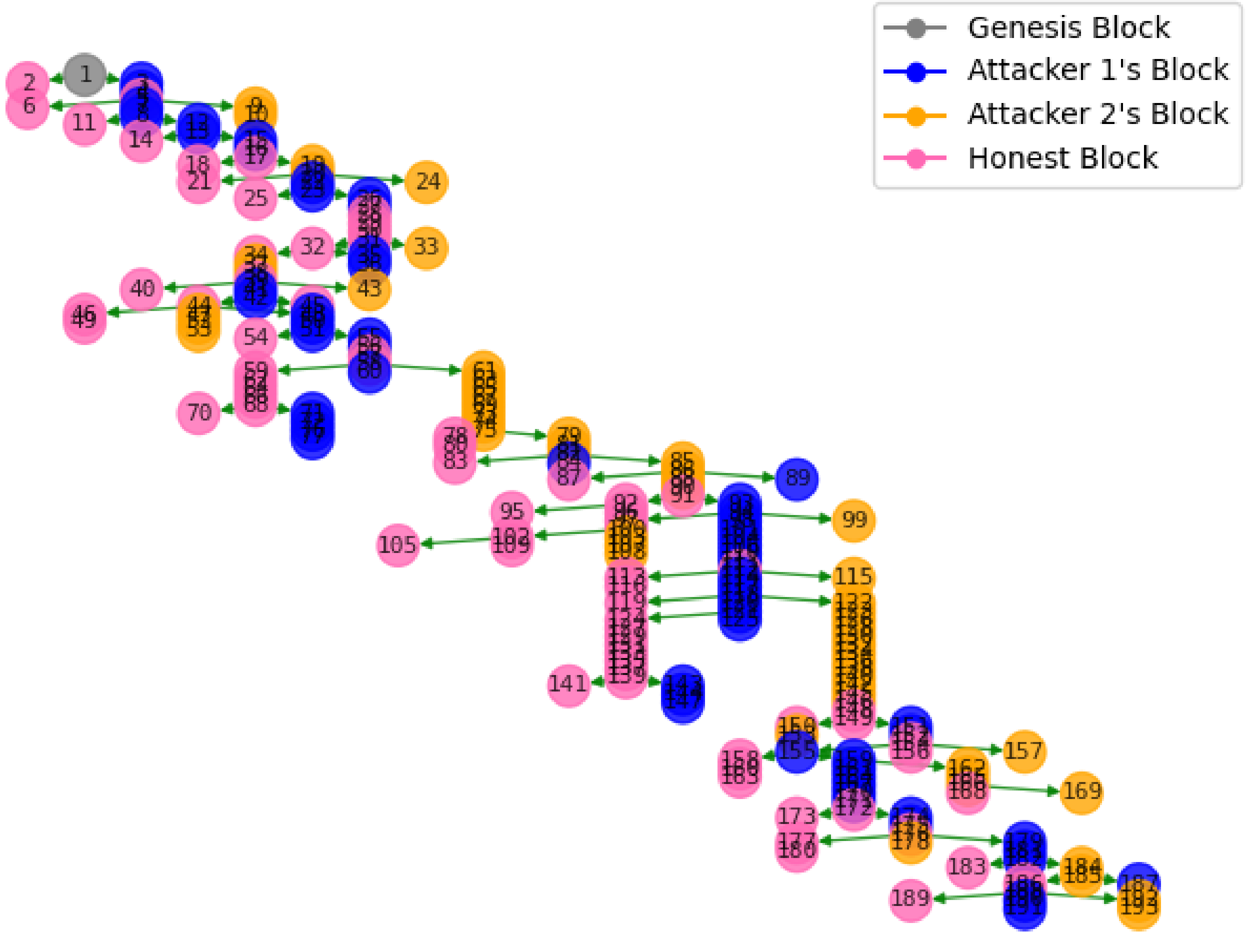

Figure 14: [Honest miner's view] Parameters: $\zeta_1 = 40$, $\zeta_2 = 30$, $I = 5$ s, $T_{sim} = 1000$ s

Category	**MPU node value**
Attacker 1	0.7419354838709677
Attacker 2	0.6071428571428571
Overall	0.5284974093264249

Table 7: MPU node statistics for parameters: $\zeta_1 = 40$, $\zeta_2 = 30$, $I = 5$ s, $T_{sim} = 1000$ s

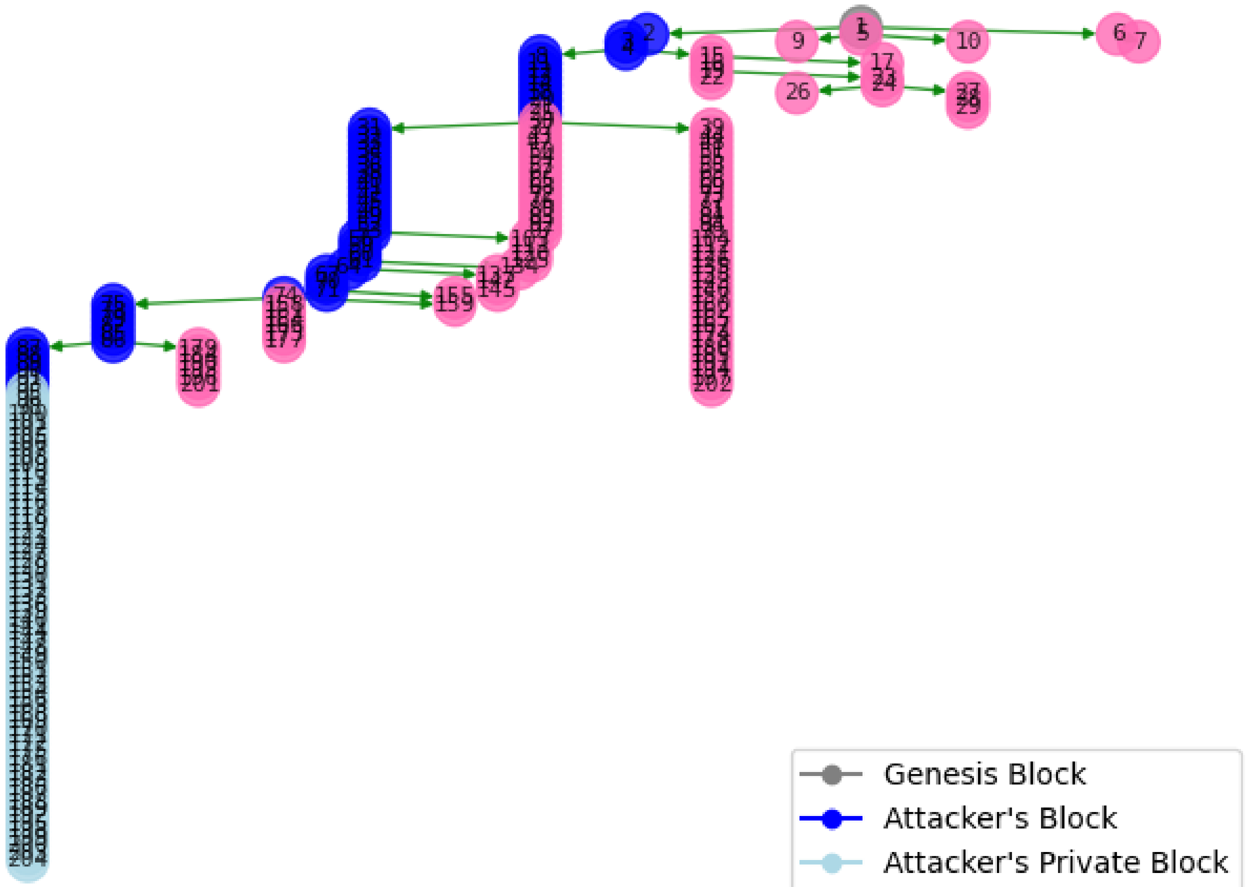

Figure 15: [Attacker-1's view] Parameters: $\zeta_1 = 50$, $\zeta_2 = 30$, $I = 5$ s, $T_{sim} = 1000$ s

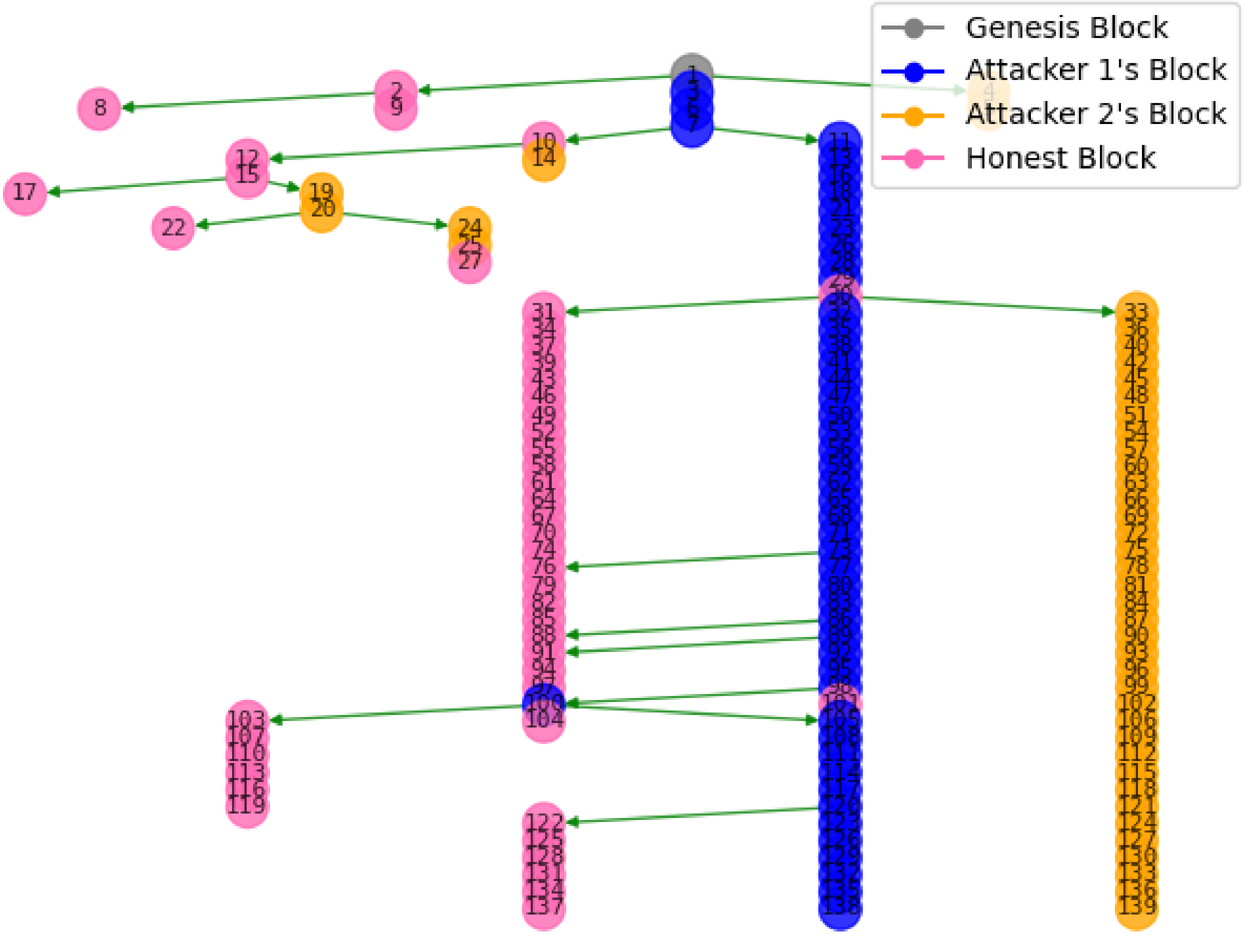

Figure 16: [Honest miner's view] Parameters: $\zeta_1 = 50$, $\zeta_2 = 30$, $I = 5$ s, $T_{sim} = 1000$ s

Category	**MPU node value**
Attacker 1	0.875
Attacker 2	0.0
Overall	0.3597122302158273

Table 8: MPU node statistics for parameters: $\zeta_1 = 50$, $\zeta_2 = 30$, $I = 5$ s, $T_{sim} = 1000$ s

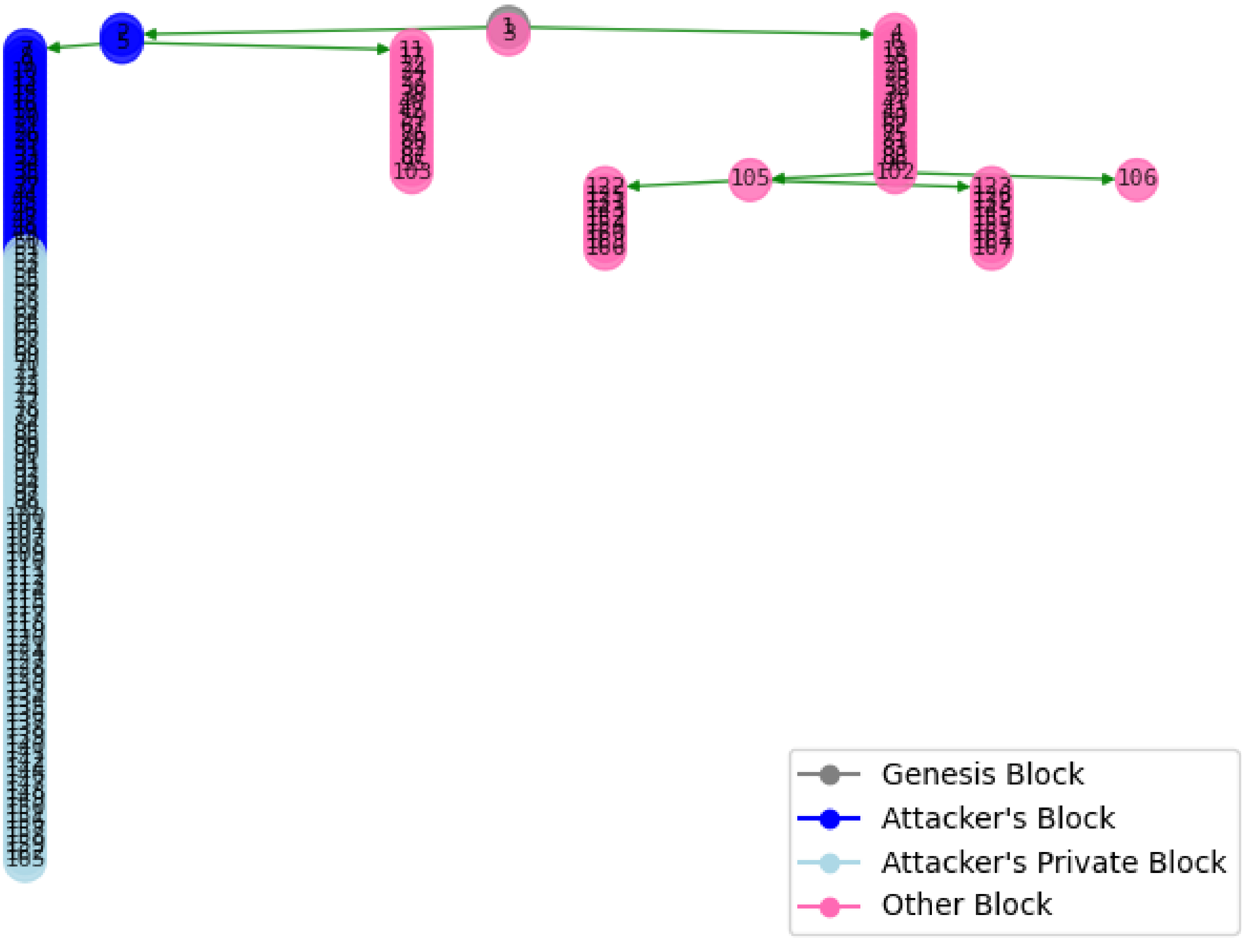

Figure 17: [Attacker-1's view] Parameters: $\zeta_1 = 60$, $\zeta_2 = 30$, $I = 5$ s, $T_{sim} = 1000$ s

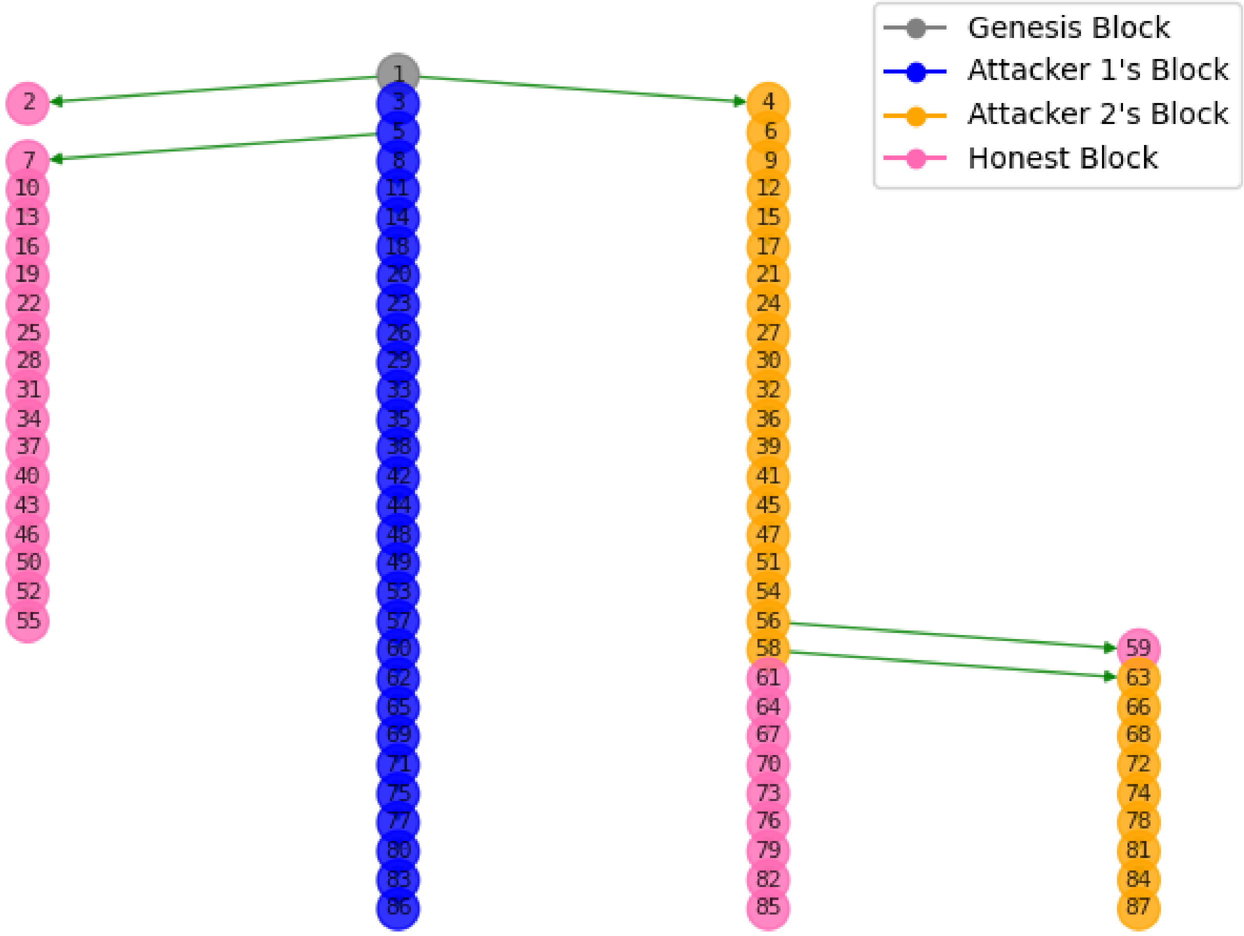

Figure 18: [Honest miner's view] Parameters: $\zeta_1 = 60$, $\zeta_2 = 30$, $I = 5$ s, $T_{sim} = 1000$ s

Category	**MPU node value**
Attacker 1	1.0
Attacker 2	0.0
Overall	0.3448275862068966

Table 9: MPU node statistics for parameters: $\zeta_1 = 60$, $\zeta_2 = 30$, $I = 5$ s, $T_{sim} = 1000$ s

2 Effect of different parameters on fraction of first attacker's block in the main chain

1. With increase in hashing power of first attacker, it's contribution to main chain increases and this ratio tends to 1. This is because with the increase in attacker's hashing power, it mostly can outpace the honest miner chain. As soon as honest nodes release a block, the attacker being in lead can release a block from its private chain hence making sure his chain is the longest chain.

2. Also, the graphs show that with increasing values of ζ_2, for the same fraction of attacker 1's attacking power, the value of fraction of first attacker's block in the main chain increases. This is because due to the nature of the attack, the attacker only needs to outpace the chain of honest miners (as the other attacker's public chain will always be at most as long as the honest chain). With increase in ζ_2, honest nodes' fraction power decreases and hence attacker is able to outpace the chain of honest miners easily.

3. Had adversaries been honest, the fraction of the attackers' block in the main chain would have been almost equal to their hashing powers, whereas by doing selfish mining attack, with the same hashing power they are now able to achieve much higher value of the fore mentioned fraction. This fraction determines the mining reward they get thus making selfish mining attack beneficial for them if they have sufficient mining power to launch the attack successfully.

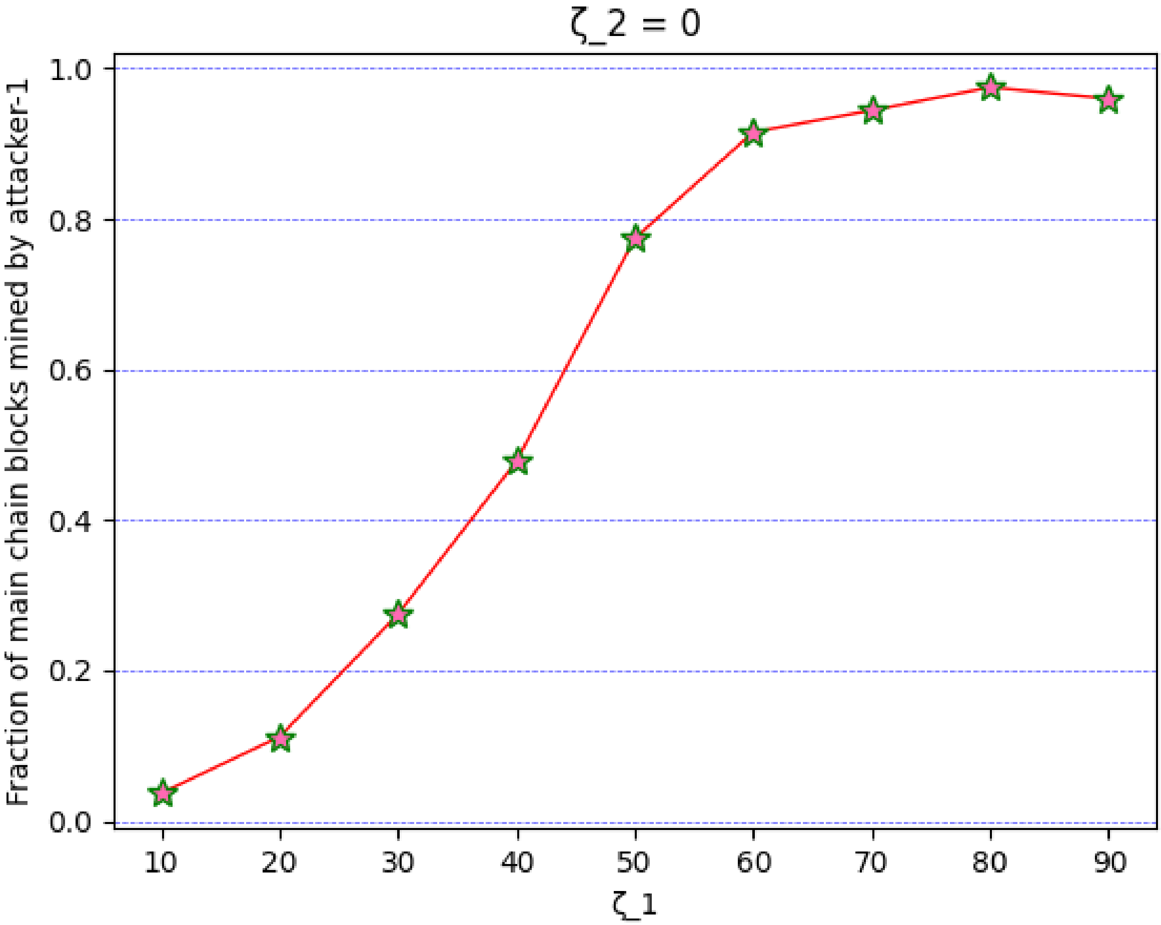

Figure 19: Parameters: $\zeta_2 = 0$, $I = 5$ s, $T_{sim} = 1000$ s

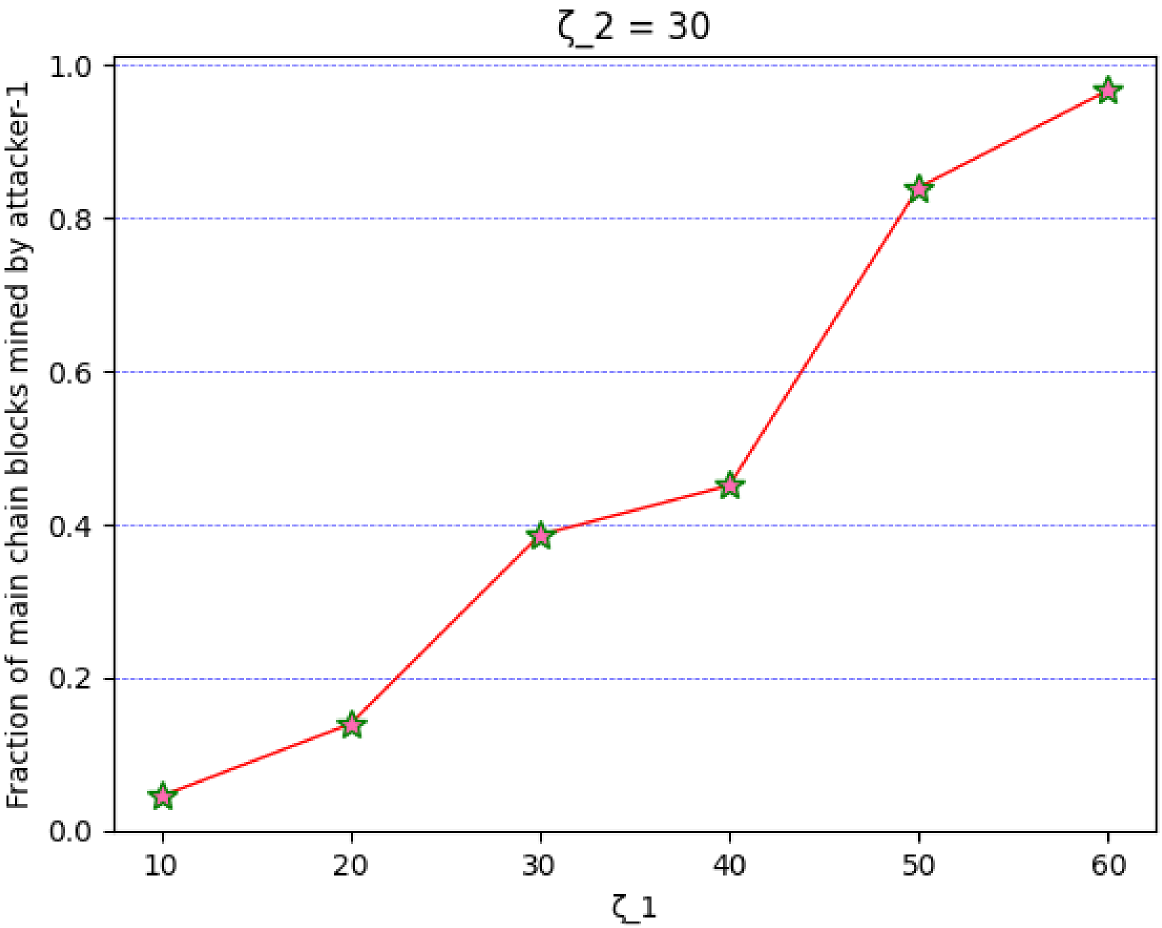

Figure 20: Parameters: $\zeta_2 = 30$, $I = 5$ s, $T_{sim} = 1000$ s

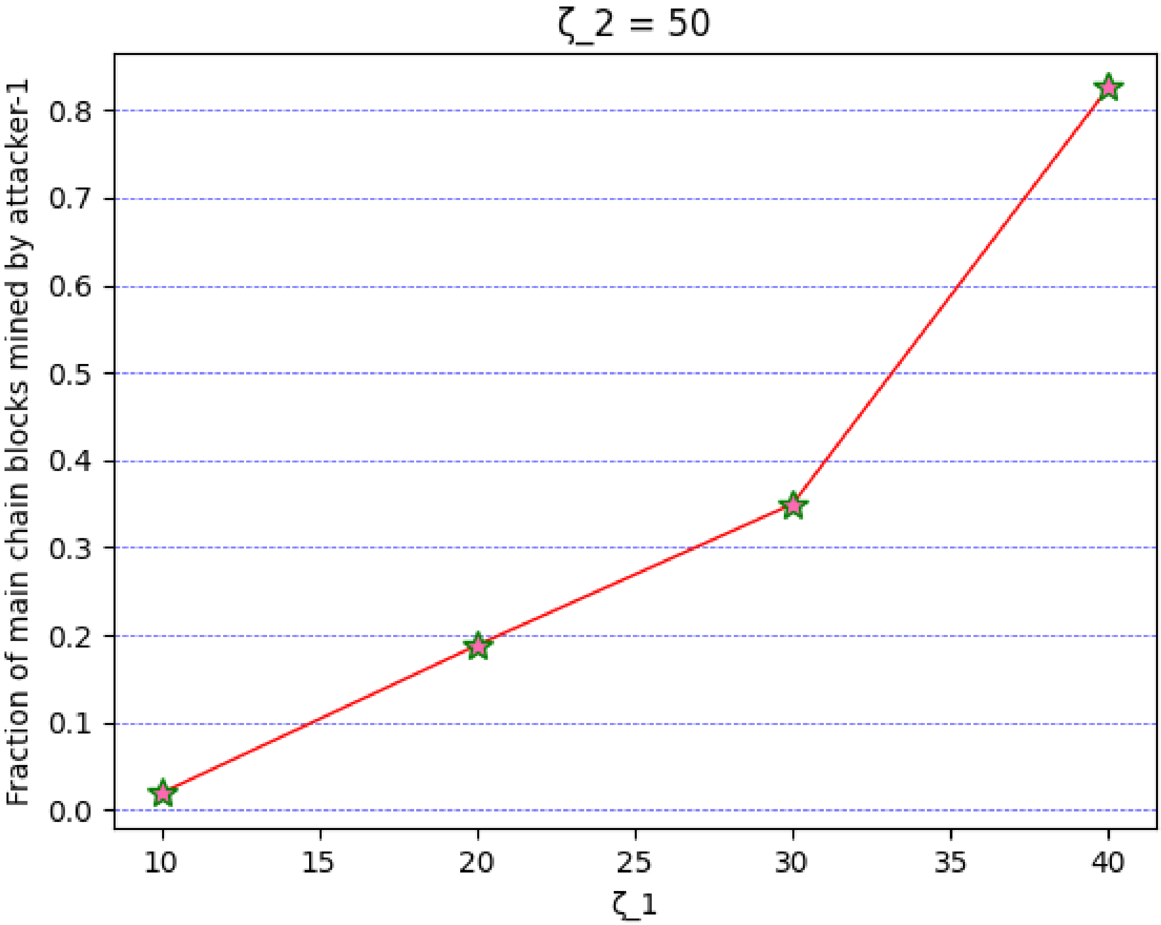

Figure 21: Parameters: $\zeta_2 = 50$, $I = 5$ s, $T_{sim} = 1000$ s

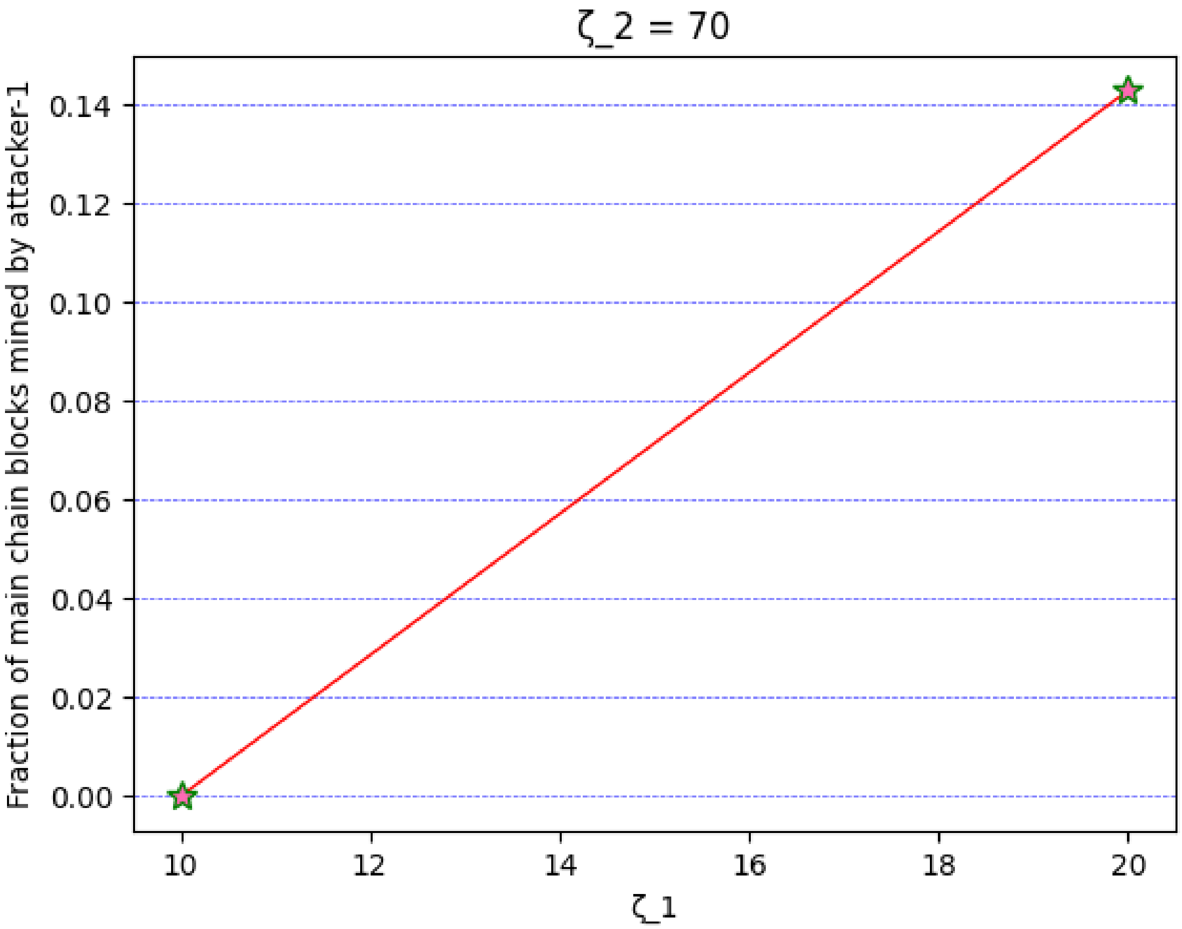

Figure 22: Parameters: $\zeta_2 = 70$, $I = 5$ s, $T_{sim} = 1000$ s