Selfish mining DAA

Boris Bukchin, Tom Yuviler

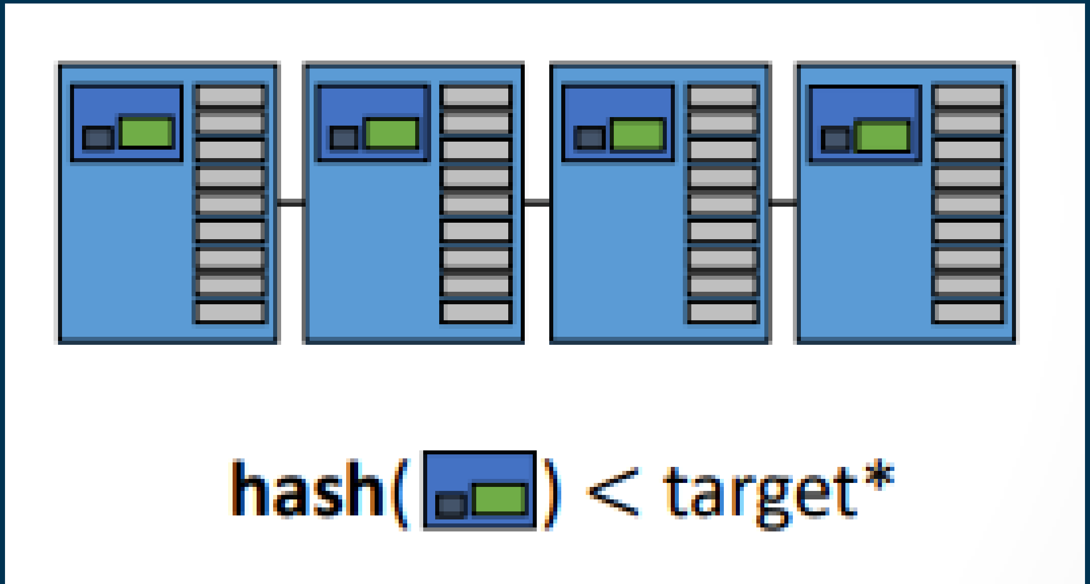
Background

Proof-of-Work

- Each miner should provide a proof-of work.
- The proportion of blocks that are generated by a miner has a direct relation with its share of hash power in the network.

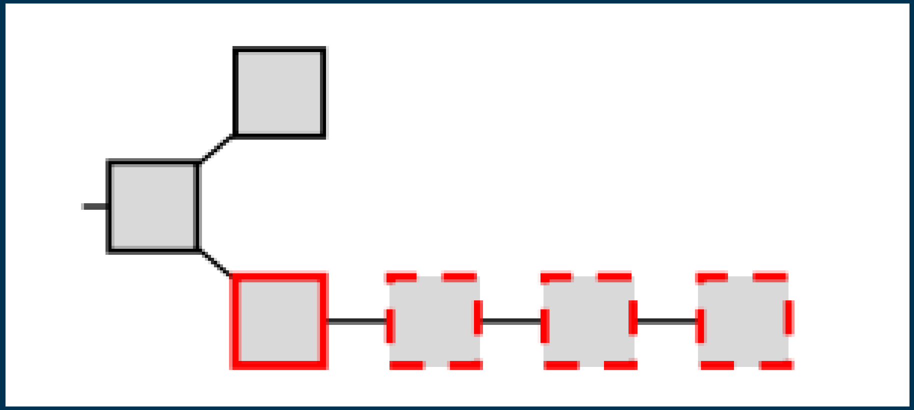
Difficulty Adjustment

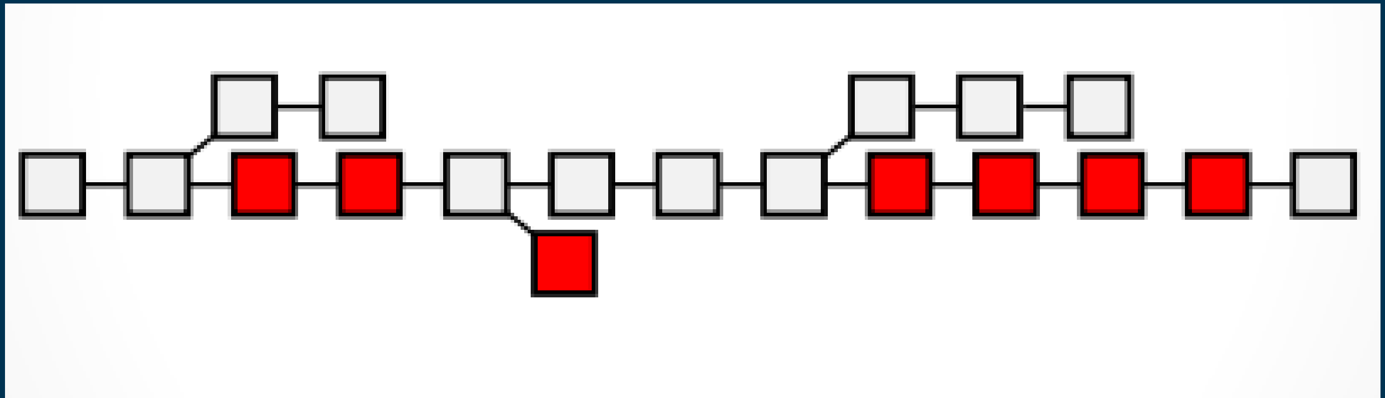
- Bitcoin block generation rate : one block every 10 minutes.
- The “target” value determines how difficult the mining process is.
  - Difficulty adjustment happens every 201 blocks (two weeks)



Selfish Mining

- Introduced by Eyal and Sirer in 2013
- Goal: Get more than fair share
  - Keep private chain
  - Intentionally fork the chain
  - Revel private chain -> waste honest nodes hash power



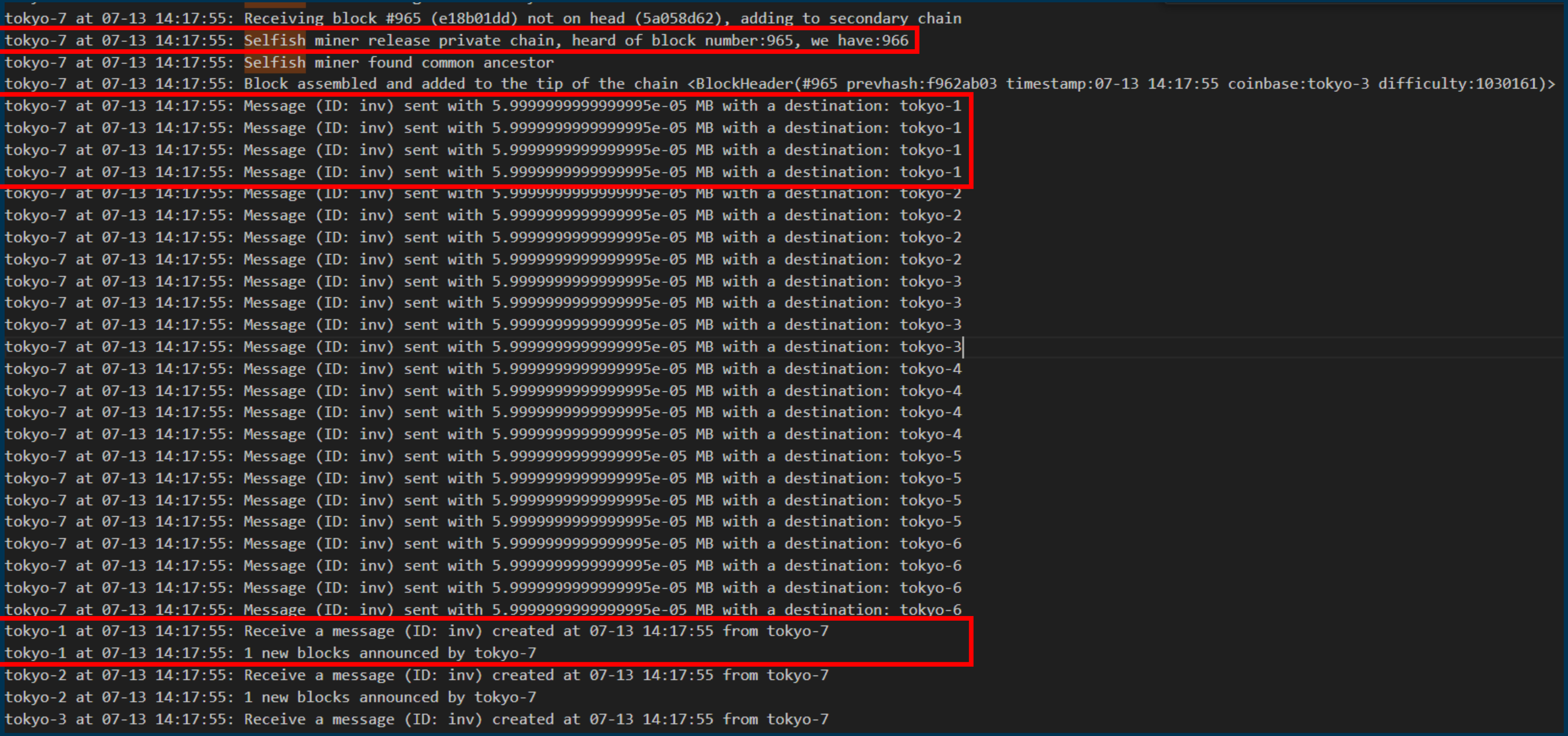


$$R_{attacker} = \frac{r_{attacker}}{r_{attacker} + r_{honest}}$$

Simulation Environment

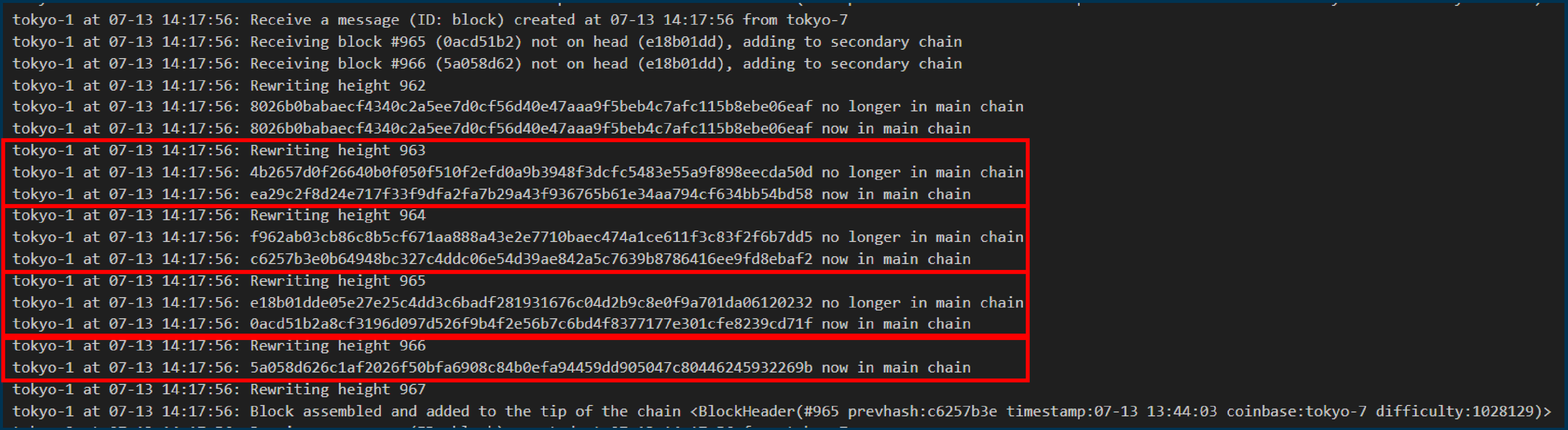
PROS	CONS
Only python	No selfish miner
Easy to understand + modify	Control only on “average time between blocks”
Fast results	Resolving forks by difficulty of the chain
	Limited amount of miners

Environment modifications - Selfish miner



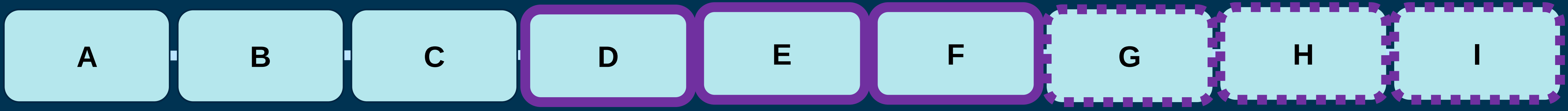
```
tokyo-7 at 07-13 14:17:55: Receiving block #965 (e18b01dd) not on head (5a058d62), adding to secondary chain
tokyo-7 at 07-13 14:17:55: Selfish miner release private chain, heard of block number:965, we have:966
tokyo-7 at 07-13 14:17:55: Selfish miner found common ancestor
tokyo-7 at 07-13 14:17:55: Block assembled and added to the tip of the chain <BlockHeader(#965 prevhash:f962ab03 timestamp:07-13 14:17:55 coinbase:tokyo-3 difficulty:1030161)>
tokyo-7 at 07-13 14:17:55: Message (ID: inv) sent with 5.9999999999999995e-05 MB with a destination: tokyo-1
tokyo-7 at 07-13 14:17:55: Message (ID: inv) sent with 5.9999999999999995e-05 MB with a destination: tokyo-1
tokyo-7 at 07-13 14:17:55: Message (ID: inv) sent with 5.9999999999999995e-05 MB with a destination: tokyo-1
tokyo-7 at 07-13 14:17:55: Message (ID: inv) sent with 5.9999999999999995e-05 MB with a destination: tokyo-1
tokyo-7 at 07-13 14:17:55: Message (ID: inv) sent with 5.9999999999999995e-05 MB with a destination: tokyo-2
tokyo-7 at 07-13 14:17:55: Message (ID: inv) sent with 5.9999999999999995e-05 MB with a destination: tokyo-2
tokyo-7 at 07-13 14:17:55: Message (ID: inv) sent with 5.9999999999999995e-05 MB with a destination: tokyo-2
tokyo-7 at 07-13 14:17:55: Message (ID: inv) sent with 5.9999999999999995e-05 MB with a destination: tokyo-2
tokyo-7 at 07-13 14:17:55: Message (ID: inv) sent with 5.9999999999999995e-05 MB with a destination: tokyo-3
tokyo-7 at 07-13 14:17:55: Message (ID: inv) sent with 5.9999999999999995e-05 MB with a destination: tokyo-3
tokyo-7 at 07-13 14:17:55: Message (ID: inv) sent with 5.9999999999999995e-05 MB with a destination: tokyo-3
tokyo-7 at 07-13 14:17:55: Message (ID: inv) sent with 5.9999999999999995e-05 MB with a destination: tokyo-3
tokyo-7 at 07-13 14:17:55: Message (ID: inv) sent with 5.9999999999999995e-05 MB with a destination: tokyo-4
tokyo-7 at 07-13 14:17:55: Message (ID: inv) sent with 5.9999999999999995e-05 MB with a destination: tokyo-4
tokyo-7 at 07-13 14:17:55: Message (ID: inv) sent with 5.9999999999999995e-05 MB with a destination: tokyo-4
tokyo-7 at 07-13 14:17:55: Message (ID: inv) sent with 5.9999999999999995e-05 MB with a destination: tokyo-4
tokyo-7 at 07-13 14:17:55: Message (ID: inv) sent with 5.9999999999999995e-05 MB with a destination: tokyo-5
tokyo-7 at 07-13 14:17:55: Message (ID: inv) sent with 5.9999999999999995e-05 MB with a destination: tokyo-5
tokyo-7 at 07-13 14:17:55: Message (ID: inv) sent with 5.9999999999999995e-05 MB with a destination: tokyo-5
tokyo-7 at 07-13 14:17:55: Message (ID: inv) sent with 5.9999999999999995e-05 MB with a destination: tokyo-5
tokyo-7 at 07-13 14:17:55: Message (ID: inv) sent with 5.9999999999999995e-05 MB with a destination: tokyo-6
tokyo-7 at 07-13 14:17:55: Message (ID: inv) sent with 5.9999999999999995e-05 MB with a destination: tokyo-6
tokyo-7 at 07-13 14:17:55: Message (ID: inv) sent with 5.9999999999999995e-05 MB with a destination: tokyo-6
tokyo-7 at 07-13 14:17:55: Message (ID: inv) sent with 5.9999999999999995e-05 MB with a destination: tokyo-6
tokyo-1 at 07-13 14:17:55: Receive a message (ID: inv) created at 07-13 14:17:55 from tokyo-7
tokyo-1 at 07-13 14:17:55: 1 new blocks announced by tokyo-7
tokyo-2 at 07-13 14:17:55: Receive a message (ID: inv) created at 07-13 14:17:55 from tokyo-7
tokyo-2 at 07-13 14:17:55: 1 new blocks announced by tokyo-7
tokyo-3 at 07-13 14:17:55: Receive a message (ID: inv) created at 07-13 14:17:55 from tokyo-7
```

Environment modifications - Longest chain protocol



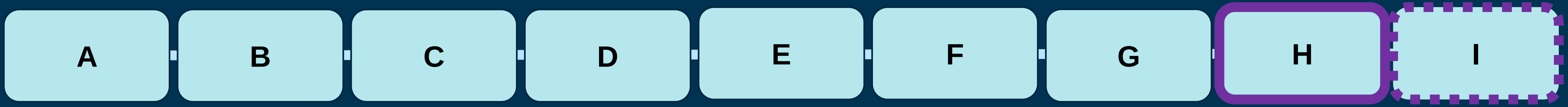
```
tokyo-1 at 07-13 14:17:56: Receive a message (ID: block) created at 07-13 14:17:56 from tokyo-7
tokyo-1 at 07-13 14:17:56: Receiving block #965 (0acd51b2) not on head (e18b01dd), adding to secondary chain
tokyo-1 at 07-13 14:17:56: Receiving block #966 (5a058d62) not on head (e18b01dd), adding to secondary chain
tokyo-1 at 07-13 14:17:56: Rewriting height 962
tokyo-1 at 07-13 14:17:56: 8026b0babaecf4340c2a5ee7d0cf56d40e47aaa9f5beb4c7afc115b8ebe06eaf no longer in main chain
tokyo-1 at 07-13 14:17:56: 8026b0babaecf4340c2a5ee7d0cf56d40e47aaa9f5beb4c7afc115b8ebe06eaf now in main chain
tokyo-1 at 07-13 14:17:56: Rewriting height 963
tokyo-1 at 07-13 14:17:56: 4b2657d0f26640b0f050f510f2efd0a9b3948f3dcfc5483e55a9f898eecda50d no longer in main chain
tokyo-1 at 07-13 14:17:56: ea29c2f8d24e717f33f9dfa2fa7b29a43f936765b61e34aa794cf634bb54bd58 now in main chain
tokyo-1 at 07-13 14:17:56: Rewriting height 964
tokyo-1 at 07-13 14:17:56: f962ab03cb86c8b5cf671aa888a43e2e7710baec474a1ce611f3c83f2f6b7dd5 no longer in main chain
tokyo-1 at 07-13 14:17:56: c6257b3e0b64948bc327c4ddc06e54d39ae842a5c7639b8786416ee9fd8ebaf2 now in main chain
tokyo-1 at 07-13 14:17:56: Rewriting height 965
tokyo-1 at 07-13 14:17:56: e18b01dde05e27e25c4dd3c6badf281931676c04d2b9c8e0f9a701da06120232 no longer in main chain
tokyo-1 at 07-13 14:17:56: 0acd51b2a8cf3196d097d526f9b4f2e56b7c6bd4f8377177e301cfe8239cd71f now in main chain
tokyo-1 at 07-13 14:17:56: Rewriting height 966
tokyo-1 at 07-13 14:17:56: 5a058d626c1af2026f50bfa6908c84b0efa94459dd905047c80446245932269b now in main chain
tokyo-1 at 07-13 14:17:56: Rewriting height 967
tokyo-1 at 07-13 14:17:56: Block assembled and added to the tip of the chain <BlockHeader(#965 prevhash:c6257b3e timestamp:07-13 13:44:03 coinbase:tokyo-7 difficulty:1028129)>
```

DAA Taxonomy: Period Based



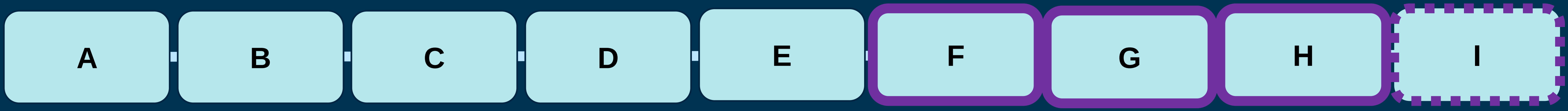
A B C D E F G H I

DAA Taxonomy: Incrementally-Extrapolated



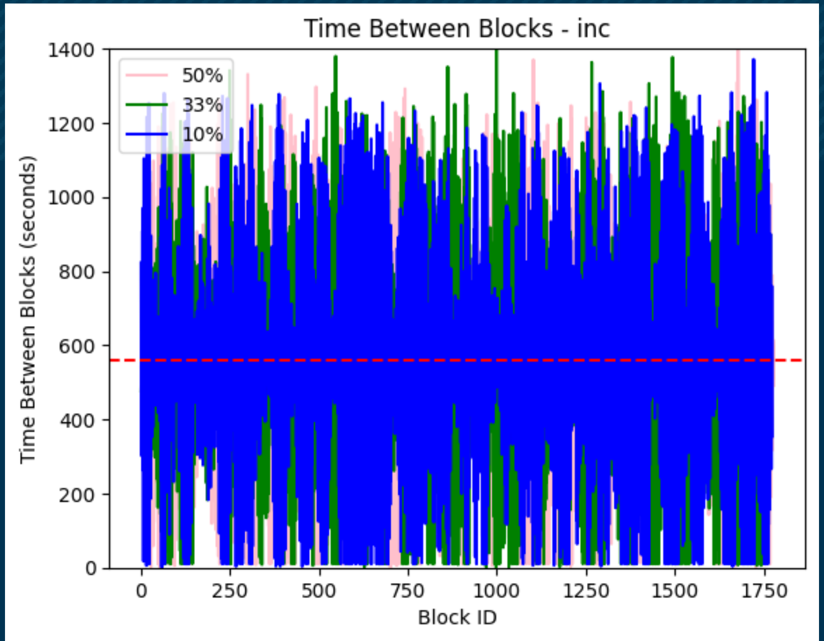
A B C D E F G H I

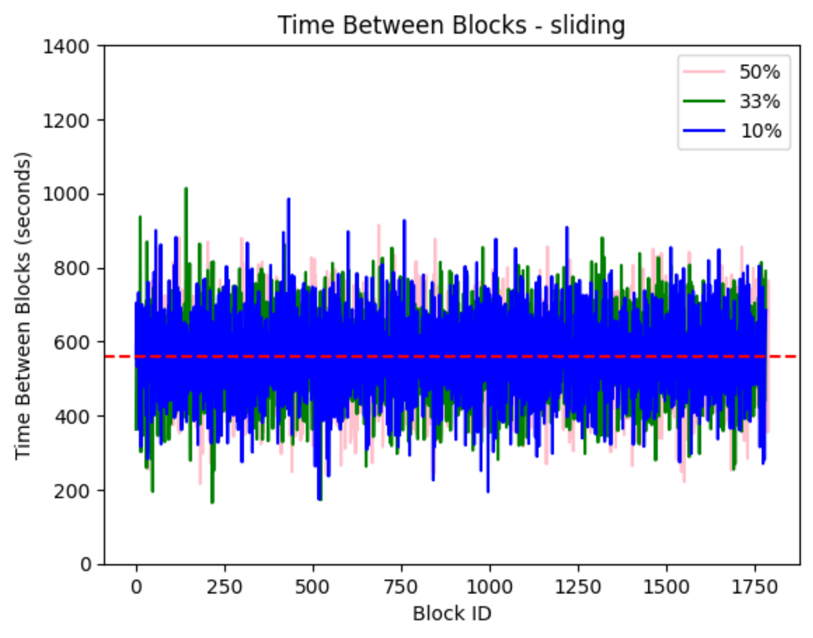
DAA Taxonomy: Sliding Window

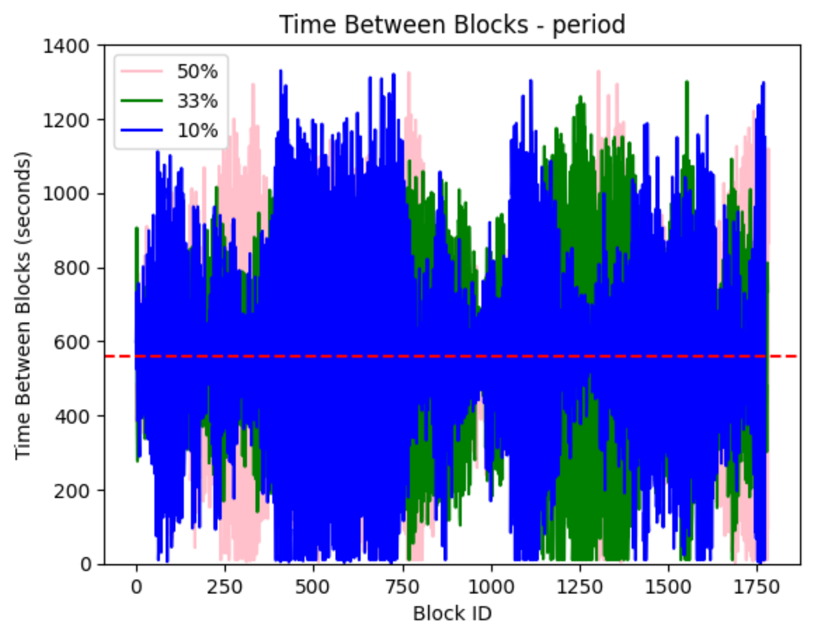


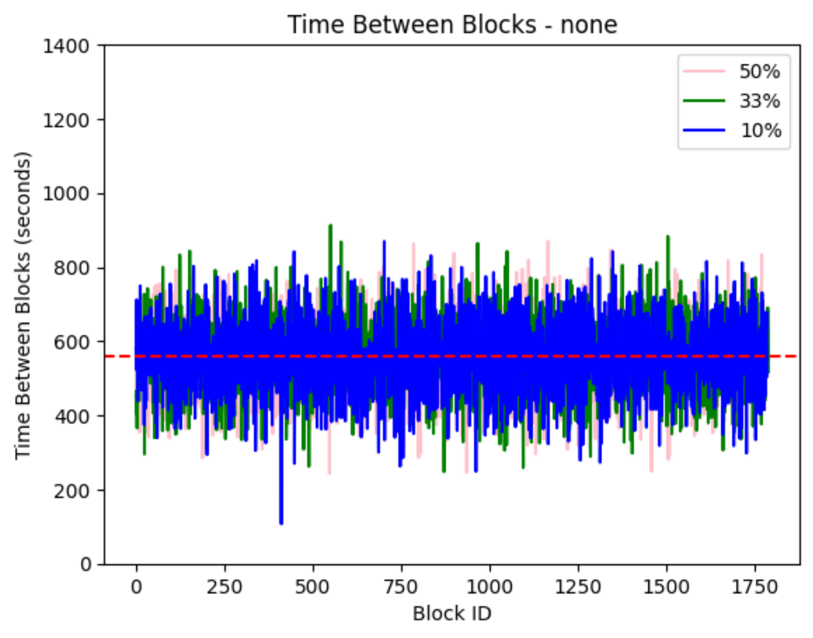
A B C D E F G H I

Results - Time Between Blocks



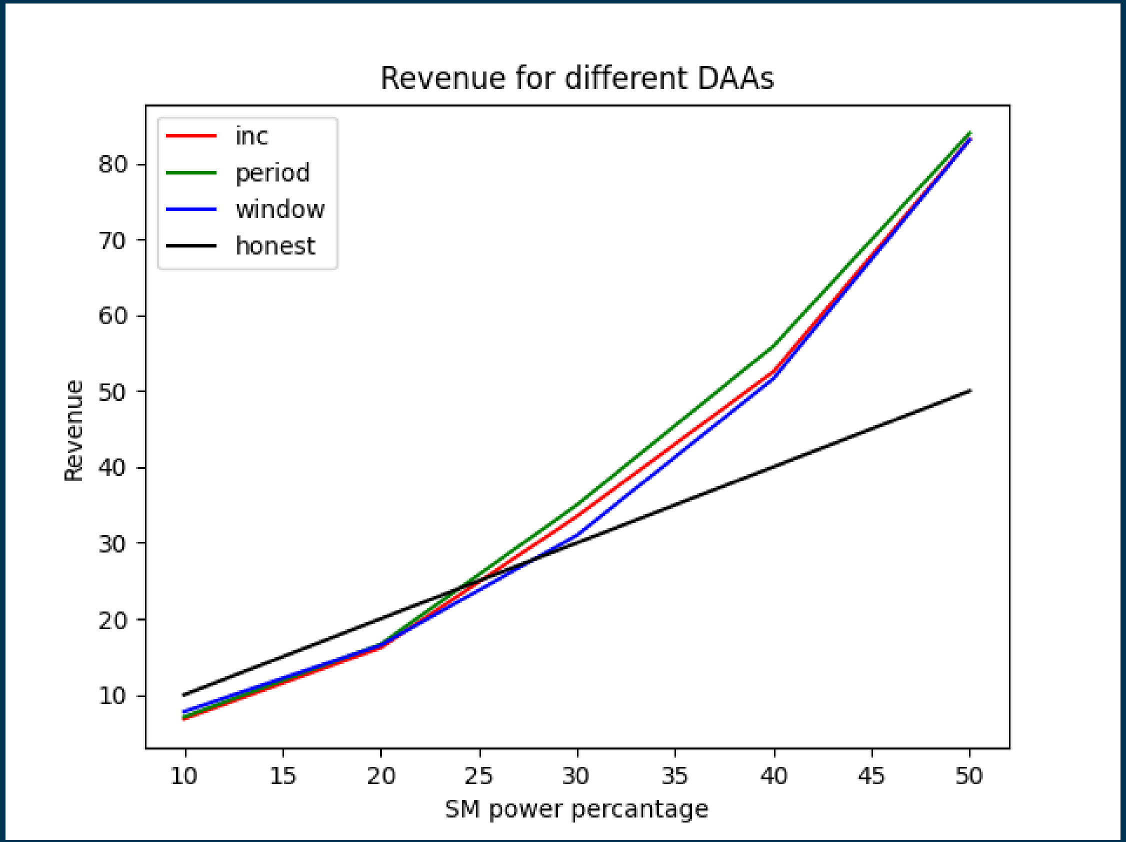




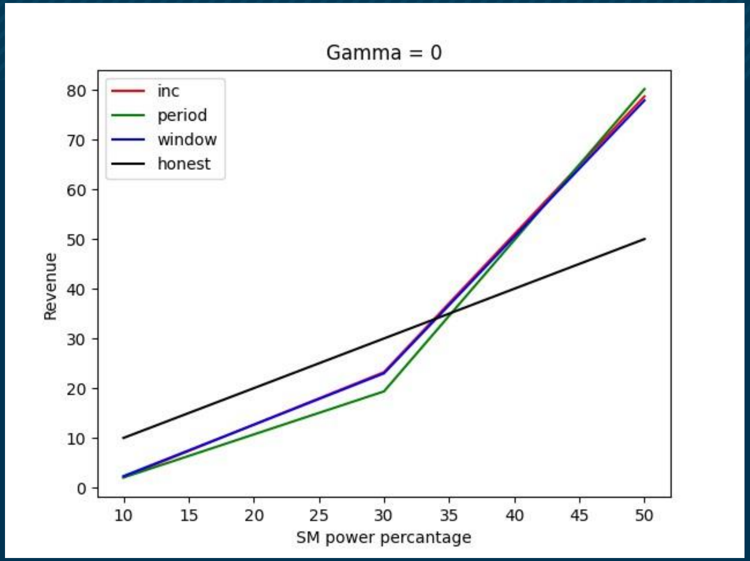


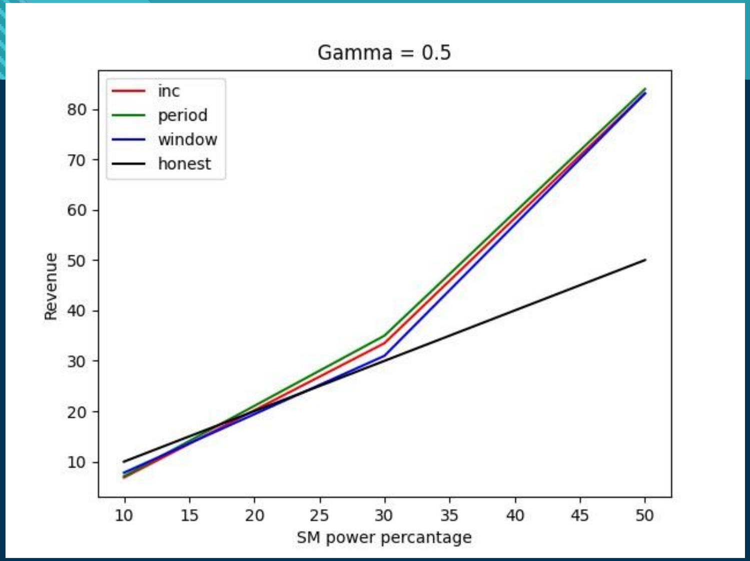
Results - DAA comparisons

~200 hours simulation length
$\gamma = 0.5$
Window size = 500

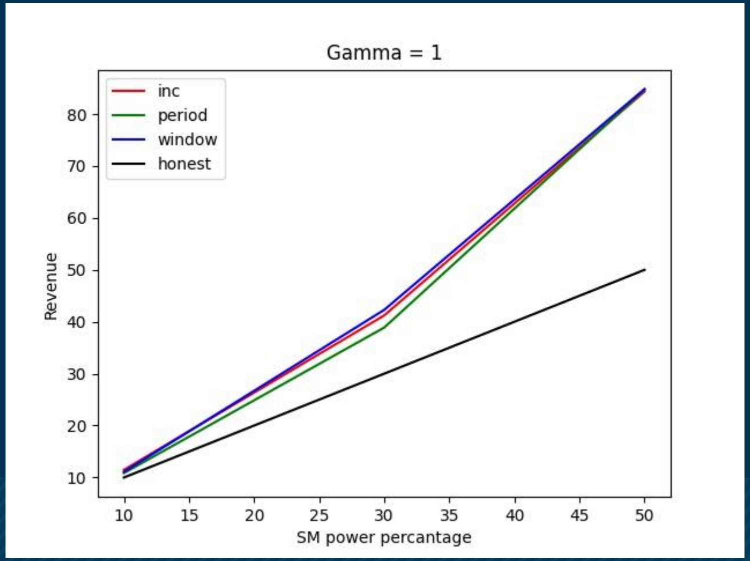


Results - γ



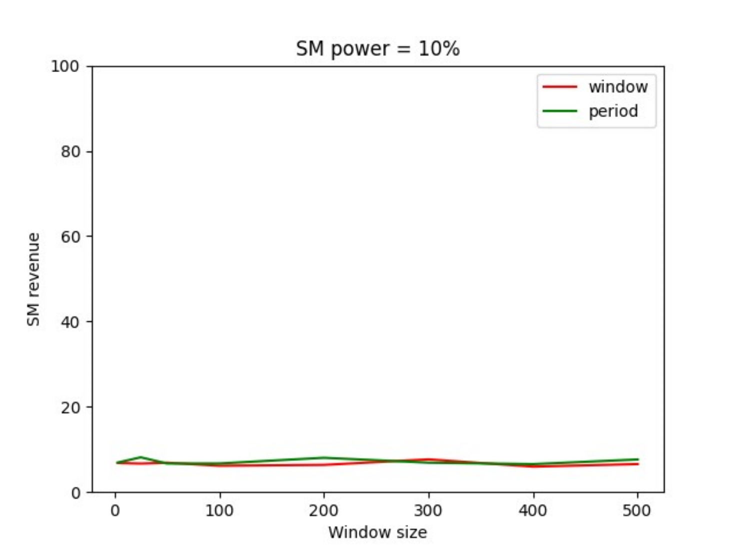


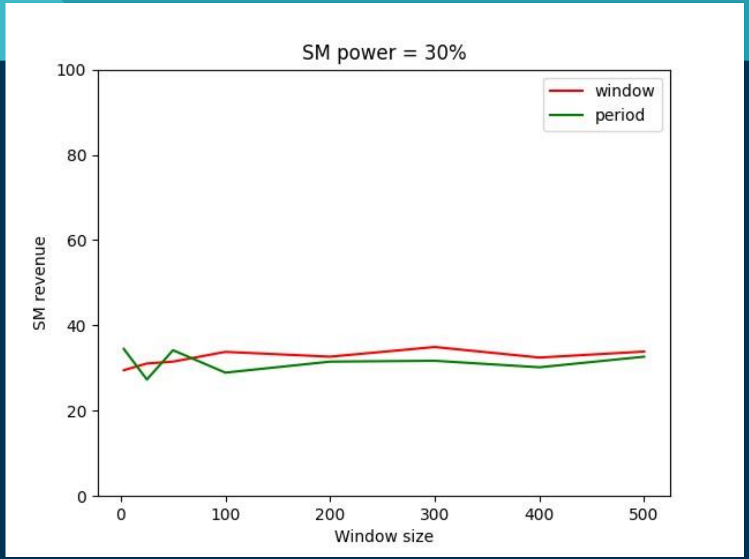
~200 hours simulation length
γ = 0.5
Window size = 500

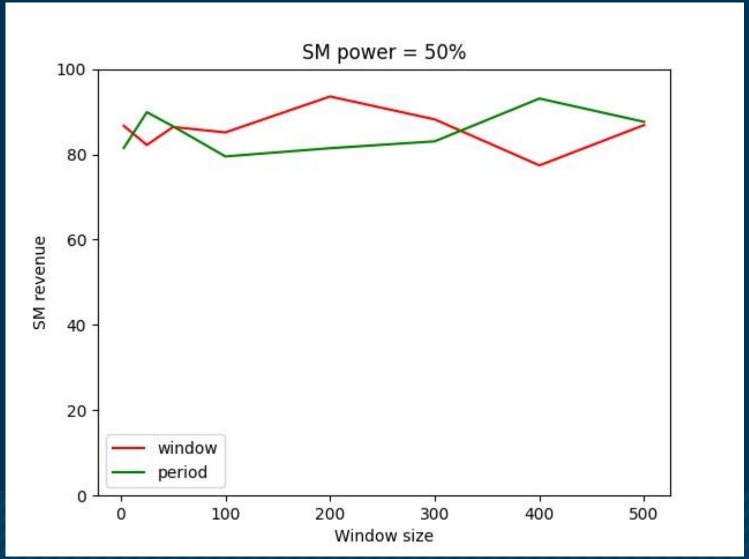


Results - Window size

~200 hours simulation length
γ = 0.5



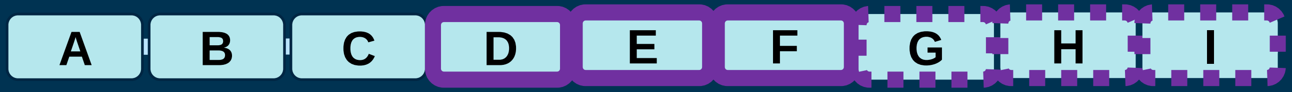




Zeno DAA

1. Period DAA:

$$D_{n-1} = D_{n-1} \times \frac{window\_size \times avarge\_time}{t_{n\times window\_size} - t_{(n-1)\times window\_size}}$$



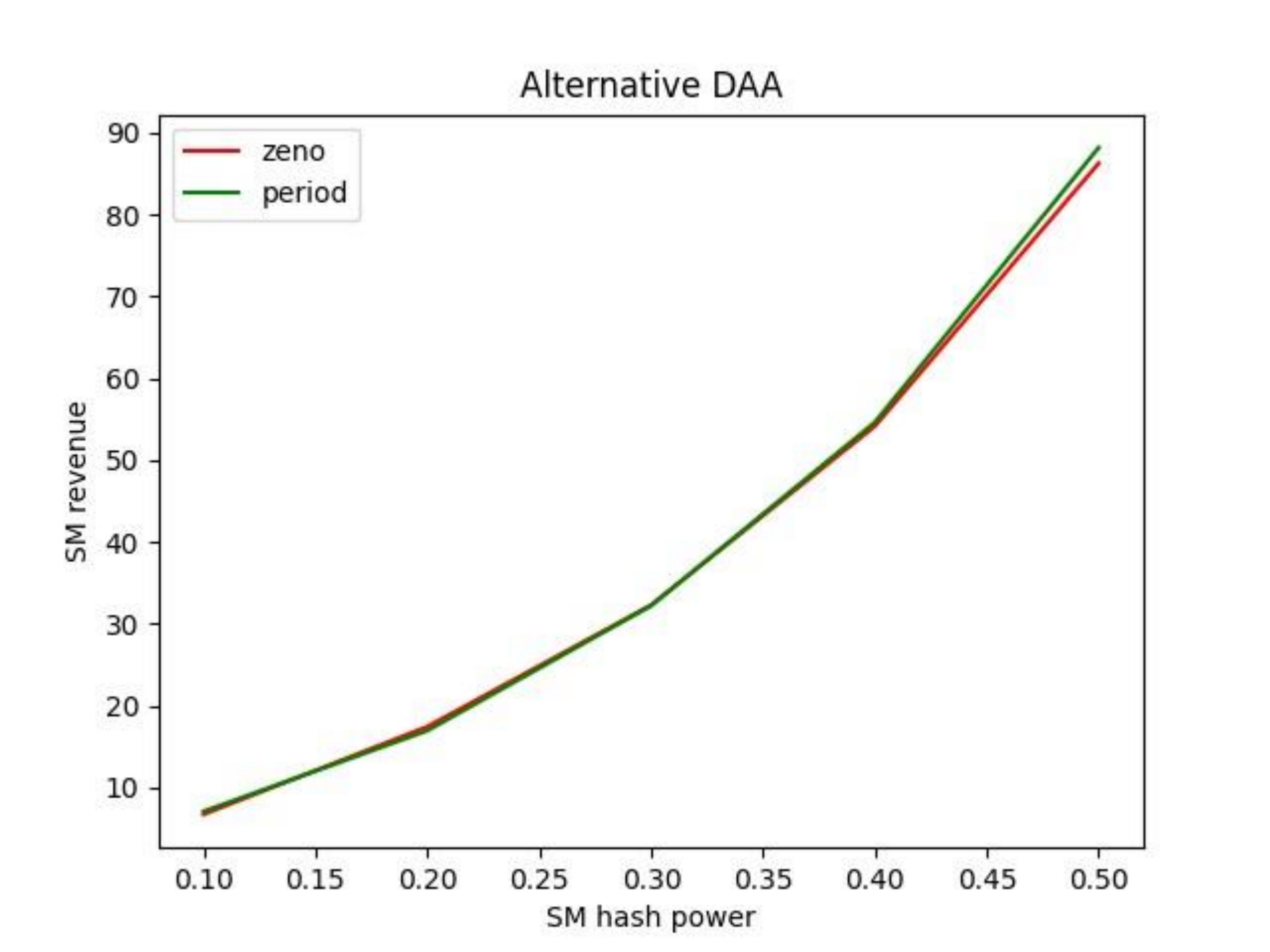
2. Zeno DAA:

$$E_{n-1} = D_{n-1} \times \frac{window\_size \times avarge\_time}{t_{n\times window\_size} - t_{(n-1)\times window\_size}}$$

$$D_n = \frac{1}{2}E_{n-1} + \frac{1}{2}D_{n-1}$$

Results - Zeno DAA

~2000 hours simulation length
γ = 0.5
Window size = 2000



Summary

- DAA as countermeasure for selfish-mining.
- Different approaches for DAA.
- Overall, selfish mining with relatively larger proportion of the hash rate can be profitable, in various scenarios of applying different difficulty adjustment algorithms.

- https://github.com/planetofwar/BlockSim

Thank You