PSet 2.0 and Difficulty Simulations

Avery Lamp and Faraaz Nadeem

Improvements to PSet 2

- Forkable
- Difficulty adjustment
- Difficulty in increments other than number of 0s
- Data endpoints

PSet 2.0

- Built with a flask server
- Uses HTTP requests and endpoints

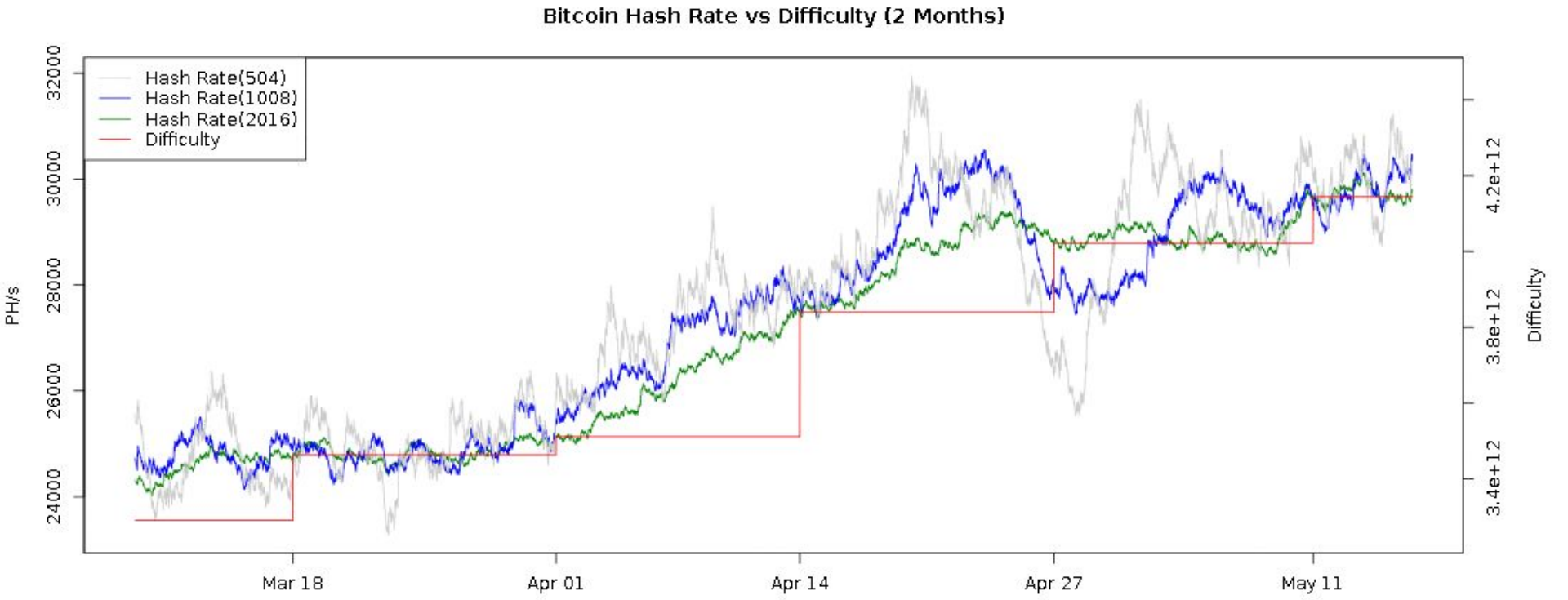
PSet 2.0 Endpoints

- **Add blocks** - /addblock/previoushash##/minername/nonce
- **Get latest** - /getlatest/
  - Returns highest block
- **Get scores** - /getscores/
  - Returns scores of all miners on main chain
- **Get all tips** - /getalltips/
  - Returns all blocks that don't have a block pointing to it
- **Get all blocks** - /getallblocks/
  - Returns all existing blocks
- **Get chain** - /getchain/<optional block hash>
  - Returns main chain, or chain from a block hash

PSet 2.0 Difficulty Adjustments

- Internal method that is easily changeable
- Different template implementations (Bitcoin, Monero)
- Made a multi-core miner that you can specify to dedicate a number of cores to mining from a specific block

Bitcoin Difficulty (avg increase 7.5%)



Bitcoin Difficulty

- Recalculated every 2016 blocks
- Has a target block duration of 10 minutes

After 2016 blocks

- Calculate hash rate of past 2016 blocks
- New difficulty is calculated to the expectation of the hash rate and two weeks time

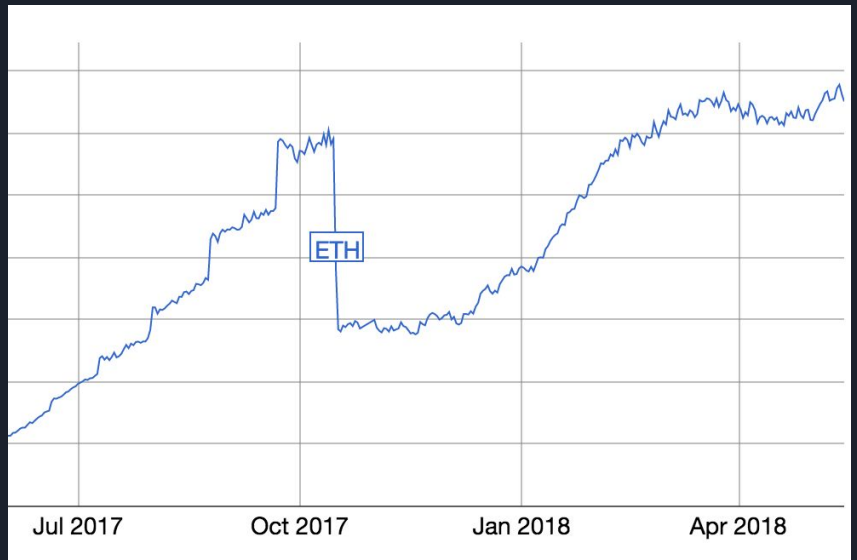
Monero Difficulty

- Average rolling window of past 720 - 120 blocks
- Discards 20% outliers (60 longest and shortest times)
- Target time of 2 minutes per block

Asic Hard Fork

Ethereum Difficulty

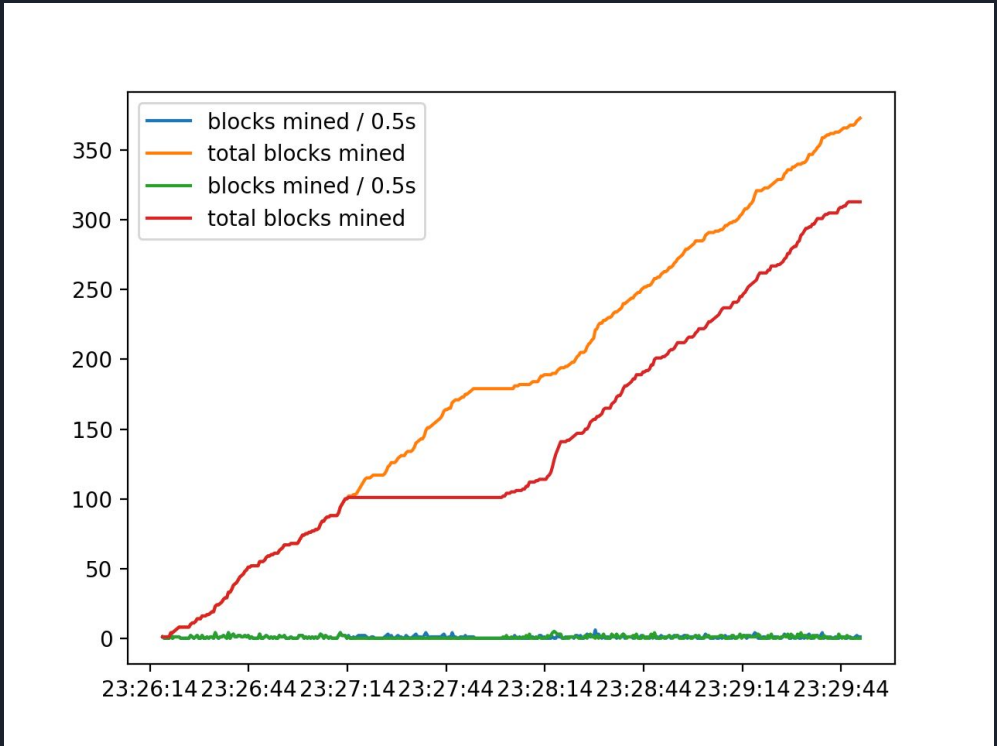
- 14 Step process for calculation
- 10-19s target
- https://dltlabs.com/how-difficulty-adjustment-algorithm-works-in-ethereum/



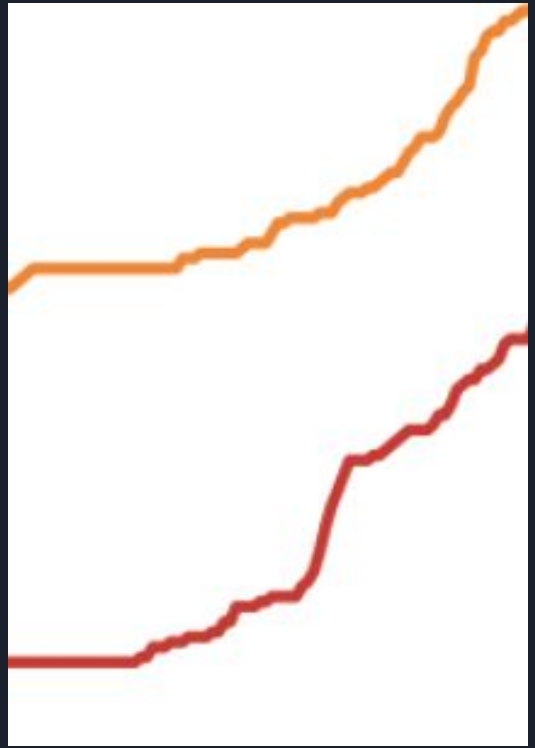
What if?

- Nodes only took the highest height
- Difficulty adjustment algorithms helped correct against 51% attacks

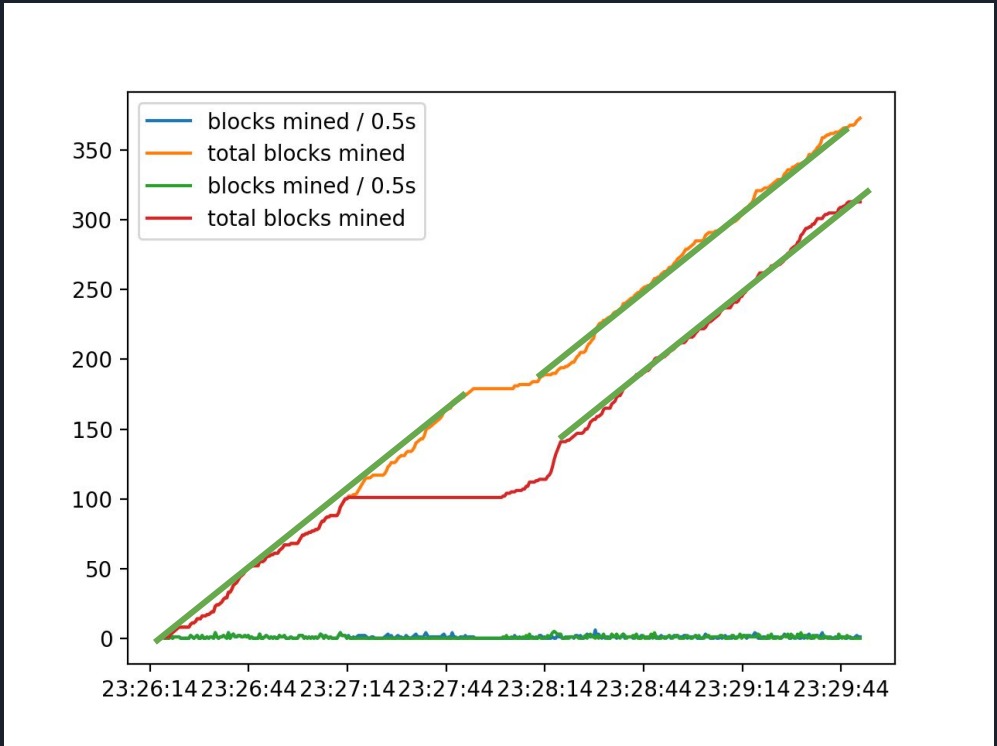
Difficulty Experimentations - (Bitcoin 30 blocks)



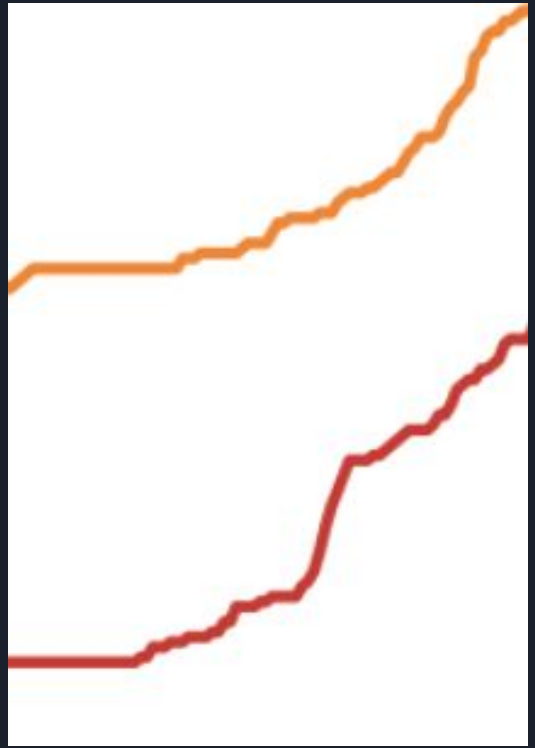
57% attack



Difficulty Experimentations - (Bitcoin 30 blocks)

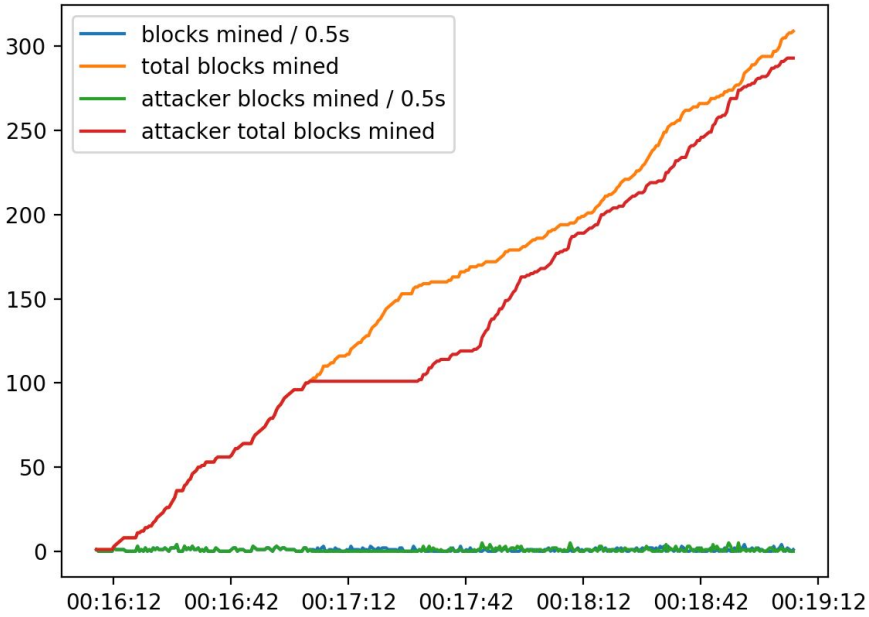


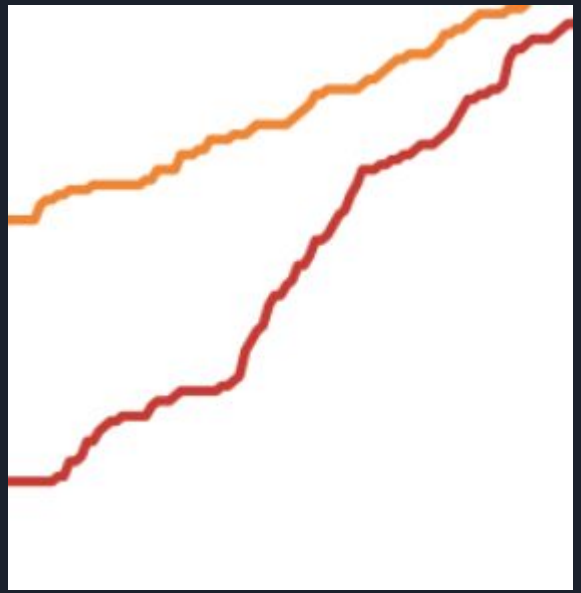
57% attack



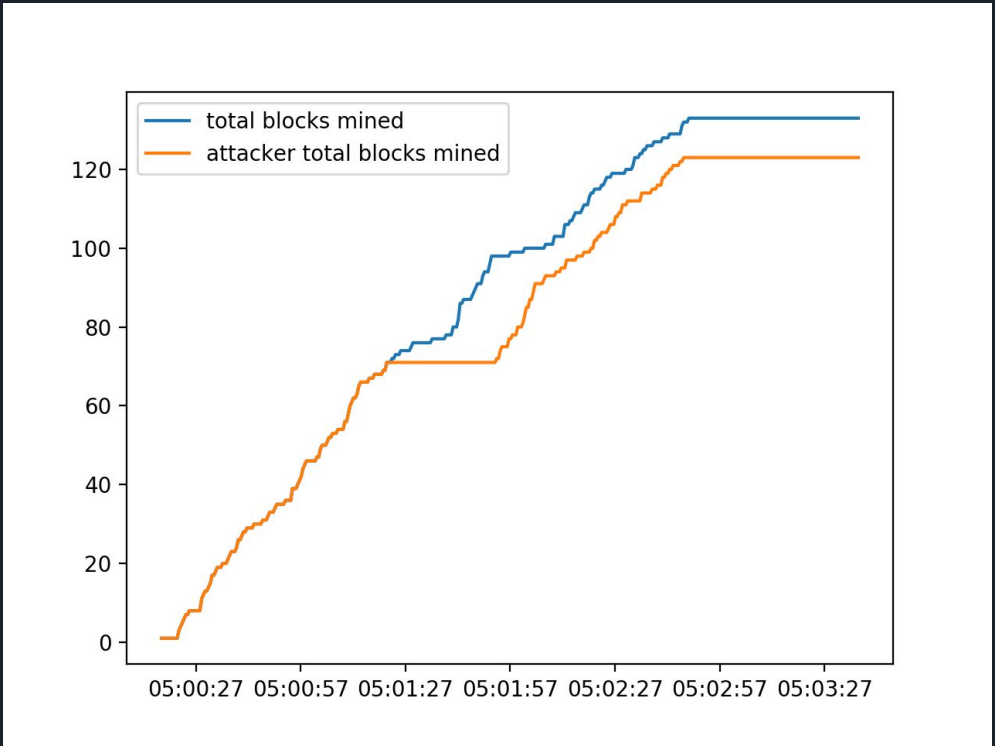
Difficulty Experimentations - (Bitcoin 30 blocks)

71% attack

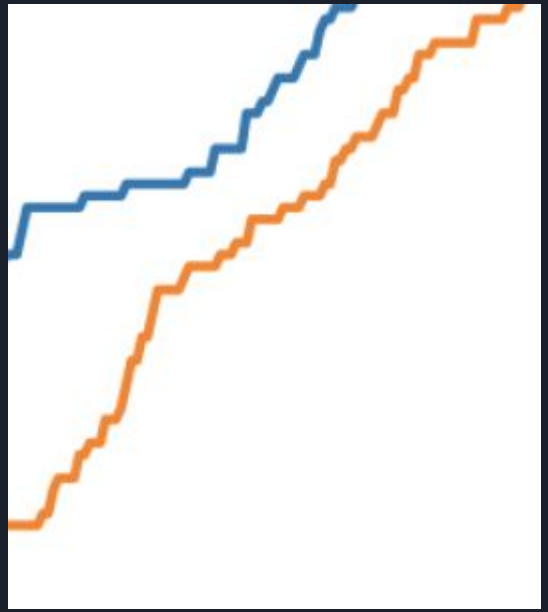




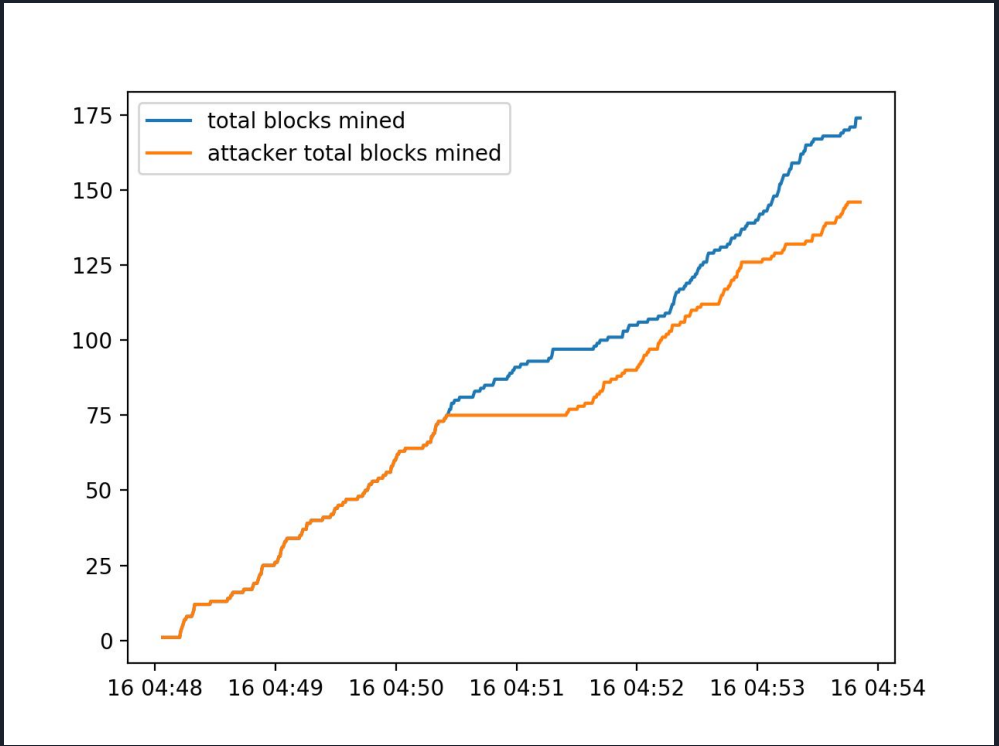
Difficulty Experimentations - (Bitcoin 10 blocks)



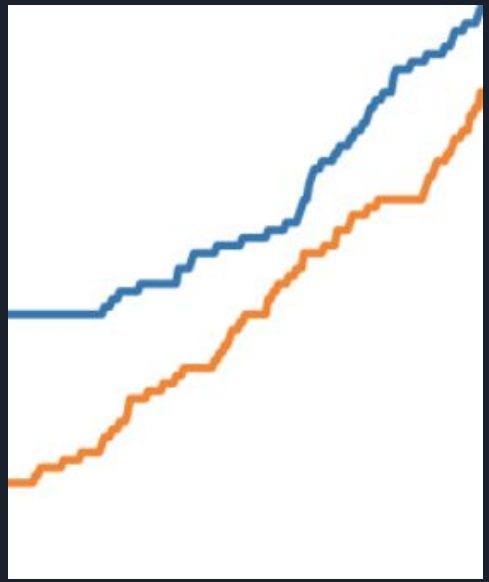
71% attack



Difficulty Experimentations
- (Monero 40 blocks 4 taken of each end)



57% attack



Problems

- Stochastic Process
- Works both ways (<51% attack)

Questions