SELFISH MINING RE-EXAMINED

Kevin Alarcón Negy[1], Peter Rizun[2], Emin Gün Sirer[1]

[1]Computer Science Department, Cornell University
[2]Bitcoin Unlimited

Bitcoin folk theorems

- Incentive compatibility
- Hash power is proportional to winnings
- Joining a mining pool does not increase chance of winning

Selfish mining

- Showed that deviant mining could be more profitable than following the Bitcoin protocol for minority miners

- The original selfish mining analysis focused only on profitability in the domain of Bitcoin

- There are ~2000 cryptocurrencies, with different difficulty adjustment algorithms

- Profitability depends on difficulty adjustment algorithm (DAA)

Critiques of selfish mining

- Over the years, critics have denied the feasibility of selfish mining with a variety of arguments

- Ignoring outlandish claims, two worth examining are:

  1. Selfish mining is unprofitable because it does not increase per time-unit profits

  2. Selfish mining must persist post-difficulty adjustment to be profitable

Our contributions

- We show that these arguments are false

- Introduce *intermittent selfish mining* strategy, which shows that a selfish miner can profit without continuing the attack past a difficulty adjustment

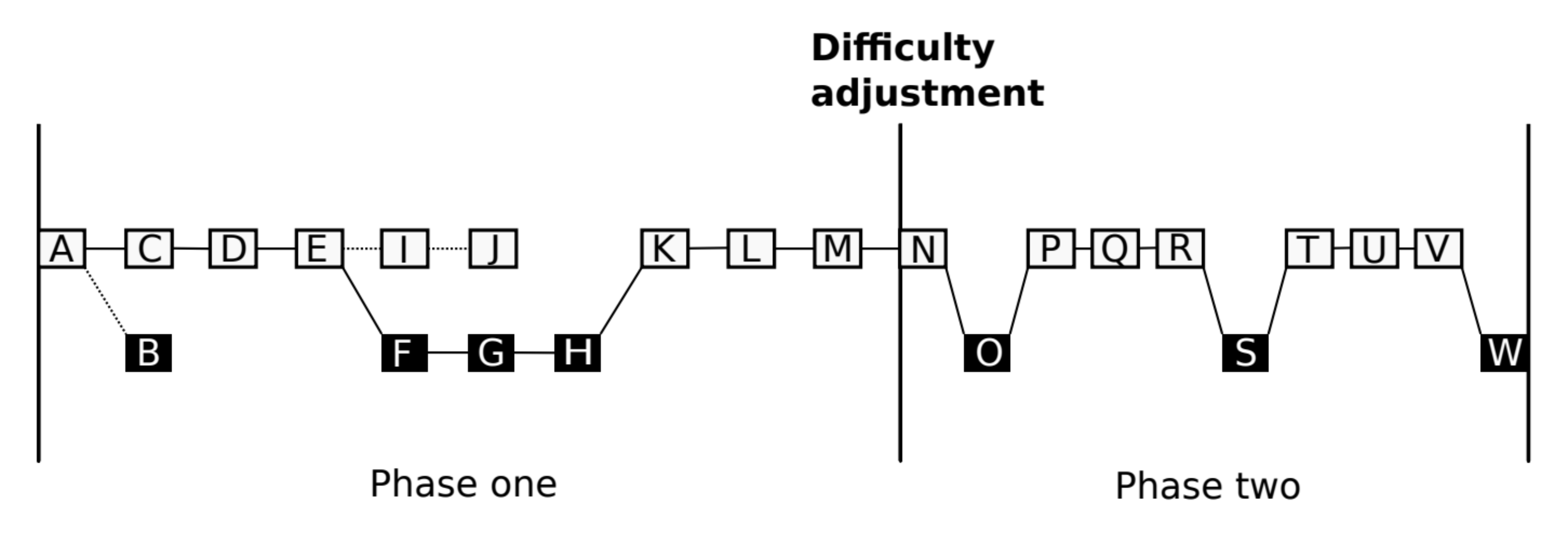
- Provide comparative analysis of BTC, ETH, XMR, and BCH/BSV DAAs

- Analyze per time-unit profitability of selfish mining with these DAAs

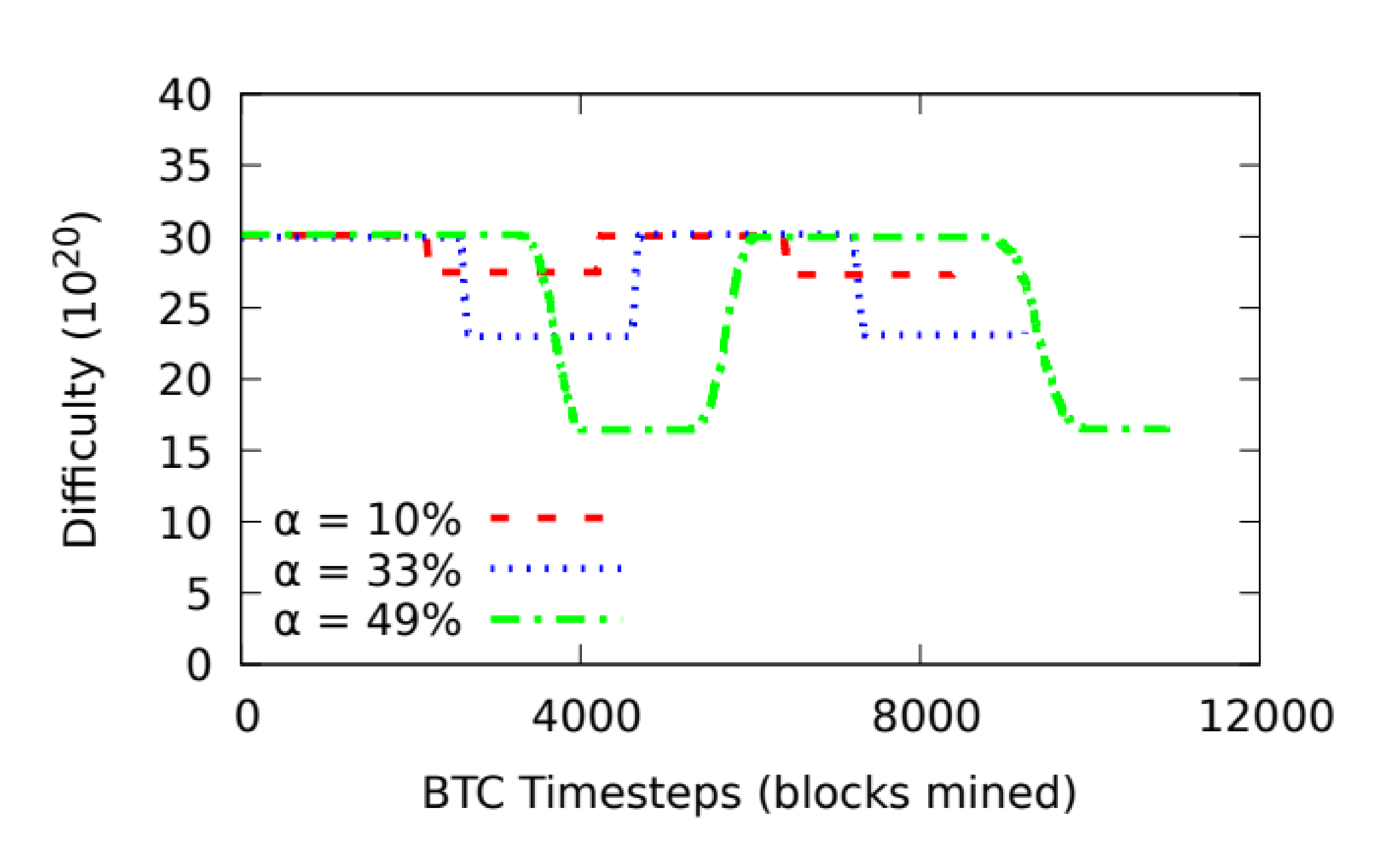
Intermittent selfish mining

- Alternate between selfish and honest mining to manipulate block difficulty
- **Phase one:** Selfishly mine to amplify time to next difficulty adjustment
- **Phase two:** Switch to honest mining to profit from lower difficulty
- Phase two benefits all miners by increase block mint rate

Intermittent selfish mining illustrated

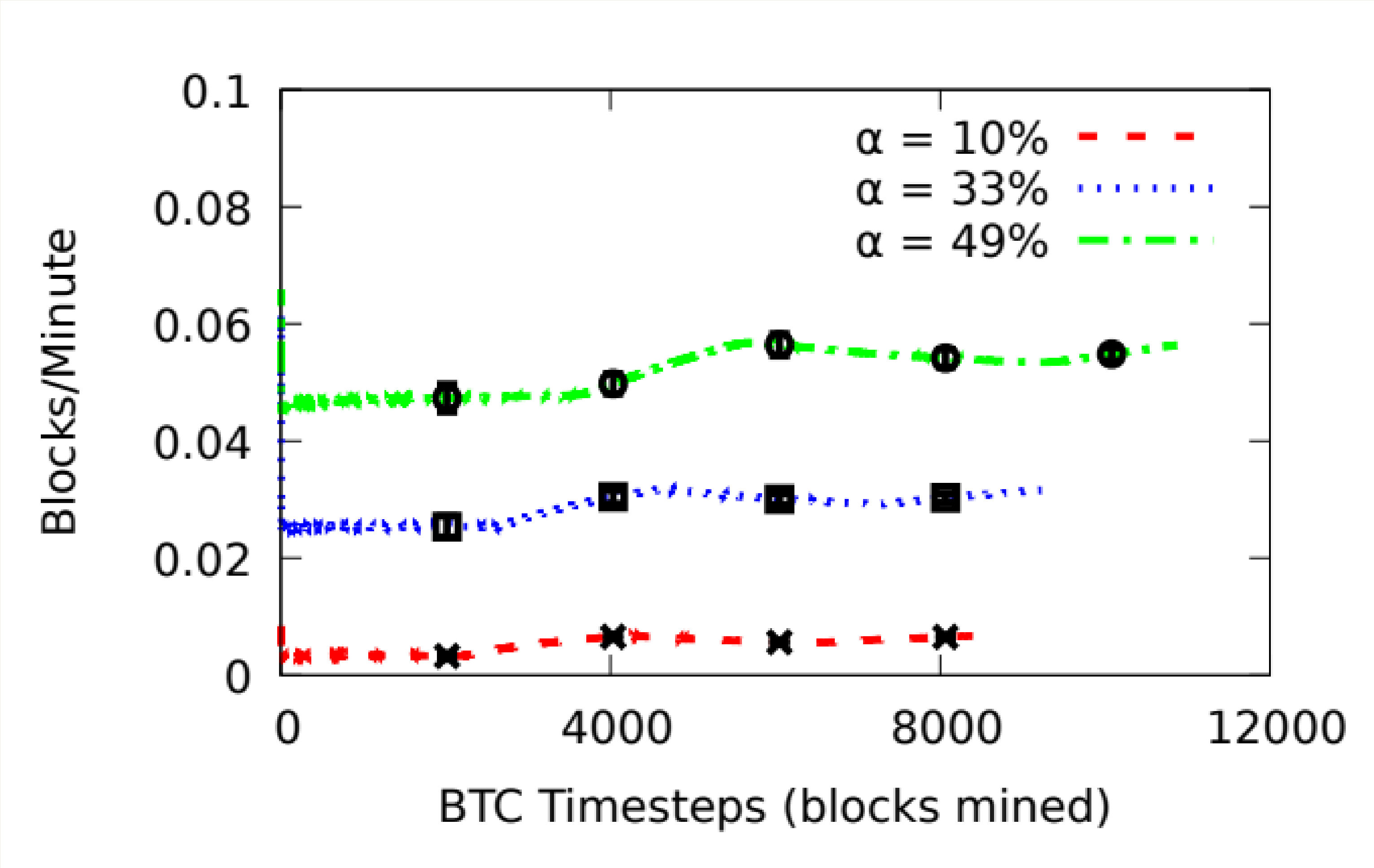


Difficulty vs. timestep



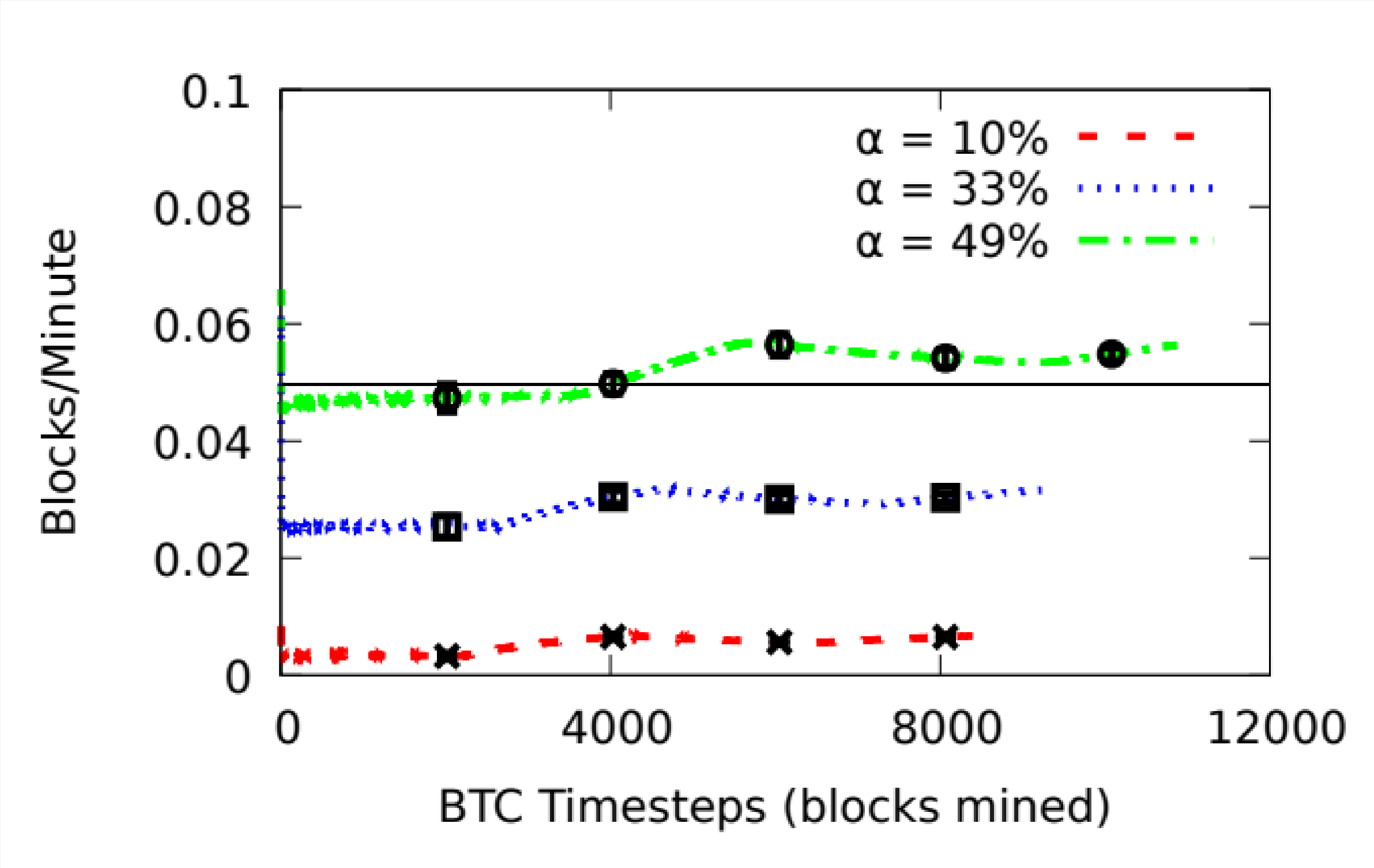
An intermittent selfish miner (ISM) causes difficulty to oscillate every adjustment period.

Block win-rate vs. timestep



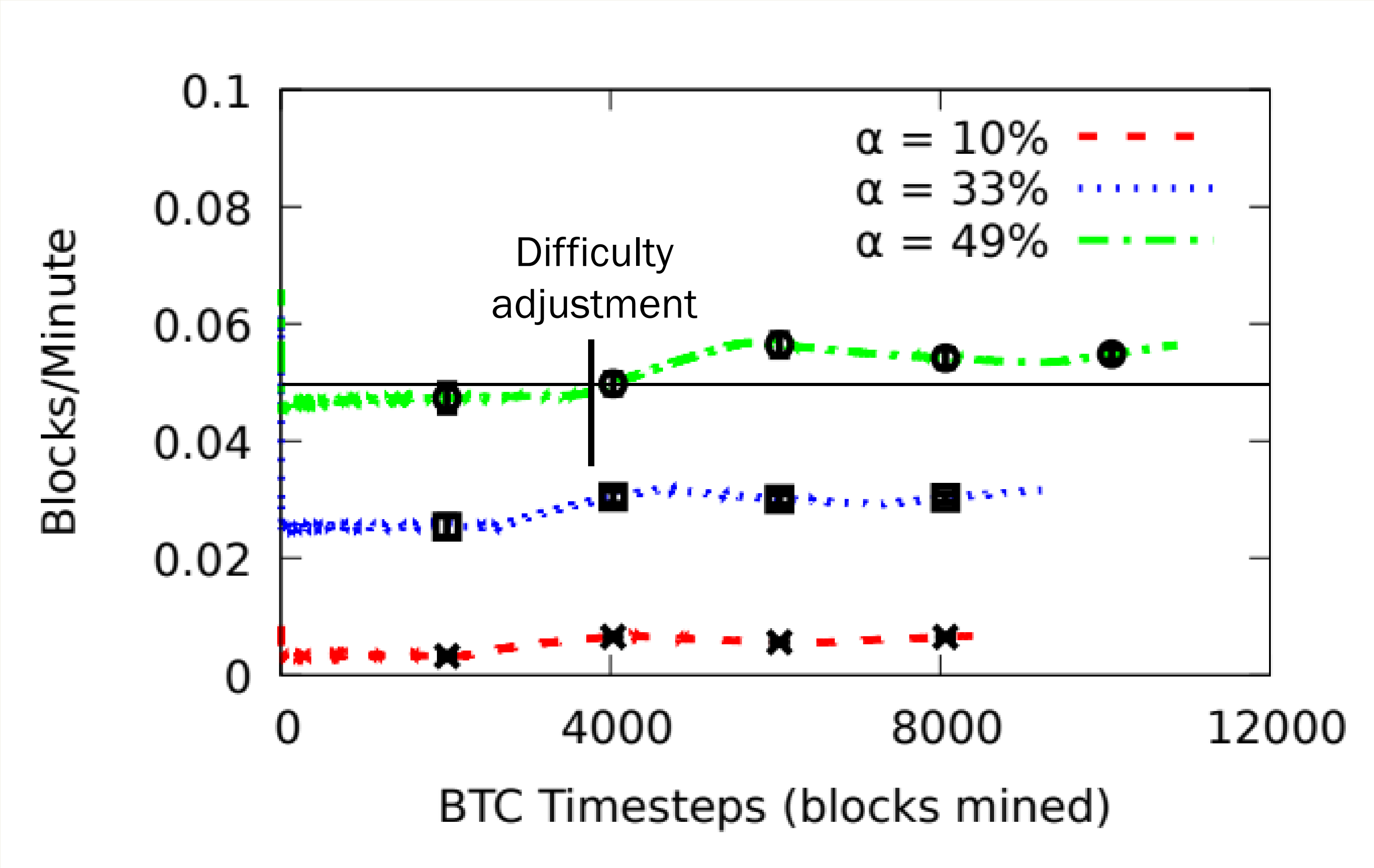
An ISM with α = 49% doubles the number of blocks to adjust difficulty, then immediately profits.

Block win-rate vs. timestep



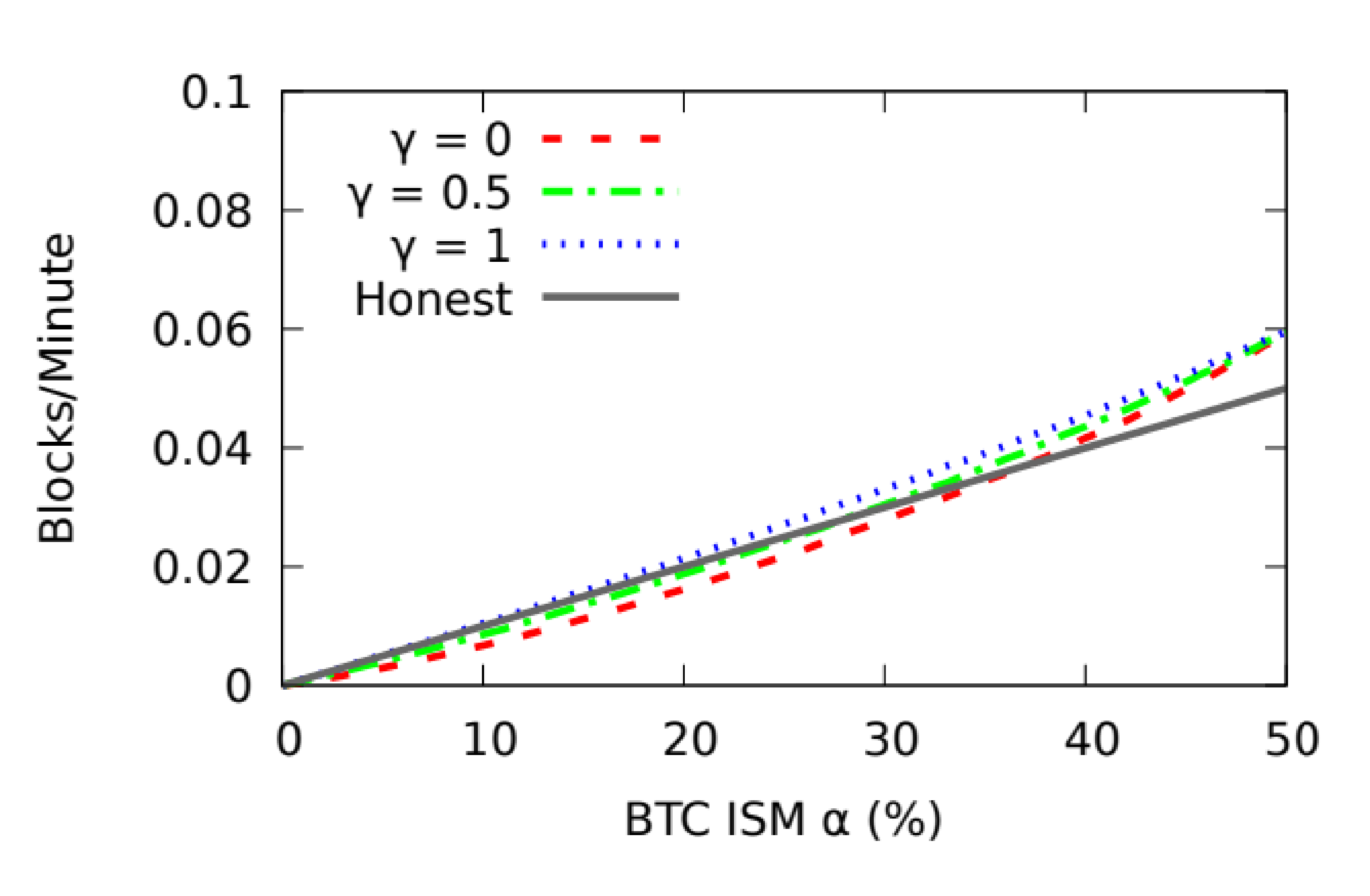
An ISM with α = 49% doubles the number of blocks to adjust difficulty, then immediately profits.

Block win-rate vs. timestep



An ISM with α = 49% doubles the number of blocks to adjust difficulty, then immediately profits.

Block win-rate vs. hash rate

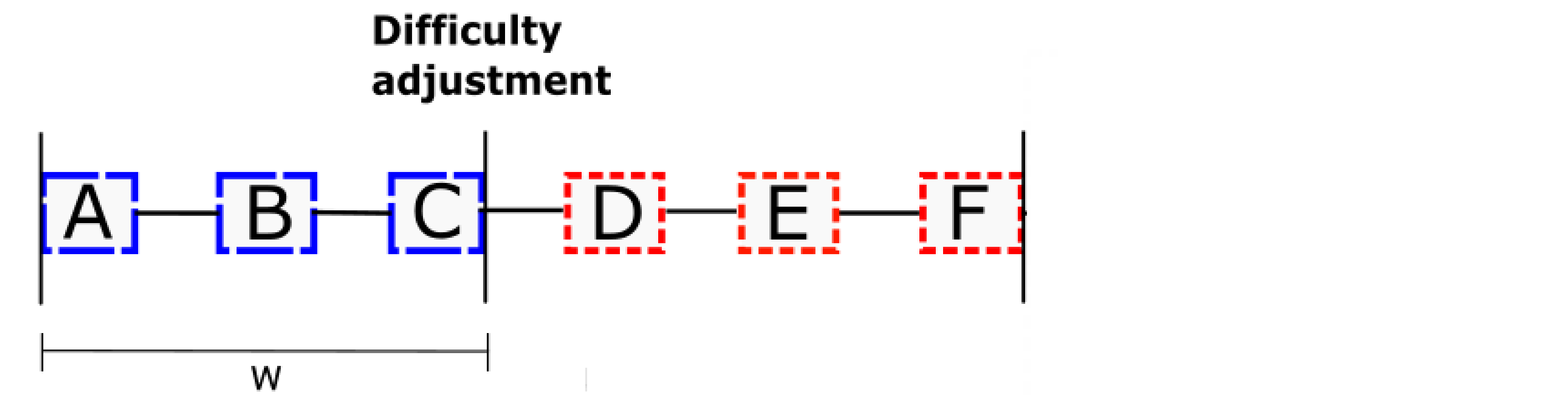


When γ = 0, an ISM with α = 37% earns more than through honest mining per time-unit.

Difficulty Adjustment Algorithm Analysis

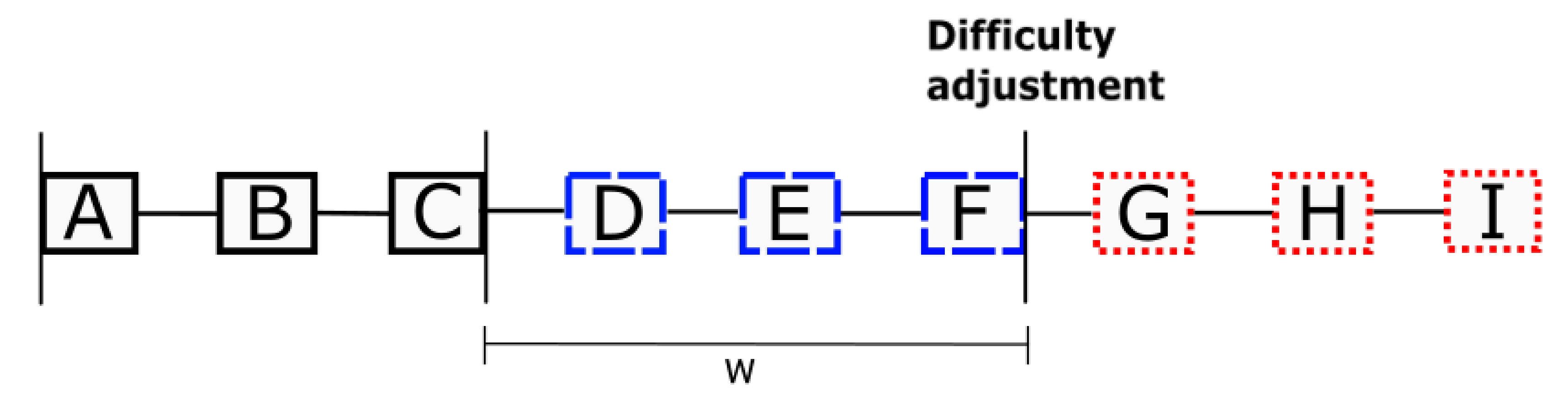
1. Period-based

- Period-based
- Incrementally-extrapolated
- Sliding-window



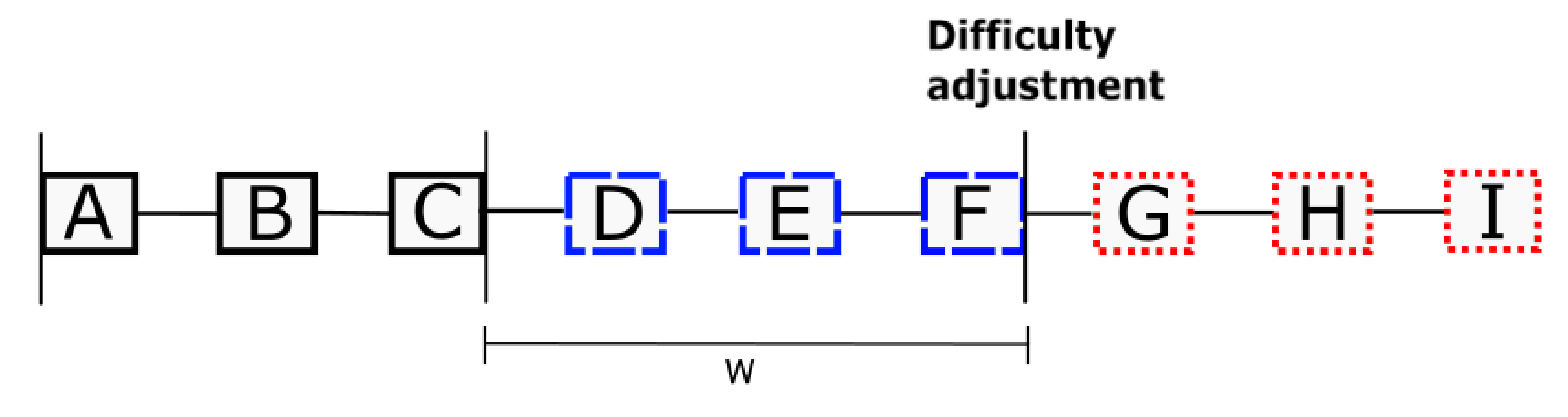
1. Period-based

- Period-based
- Incrementally-extrapolated
- Sliding-window



1. Period-based

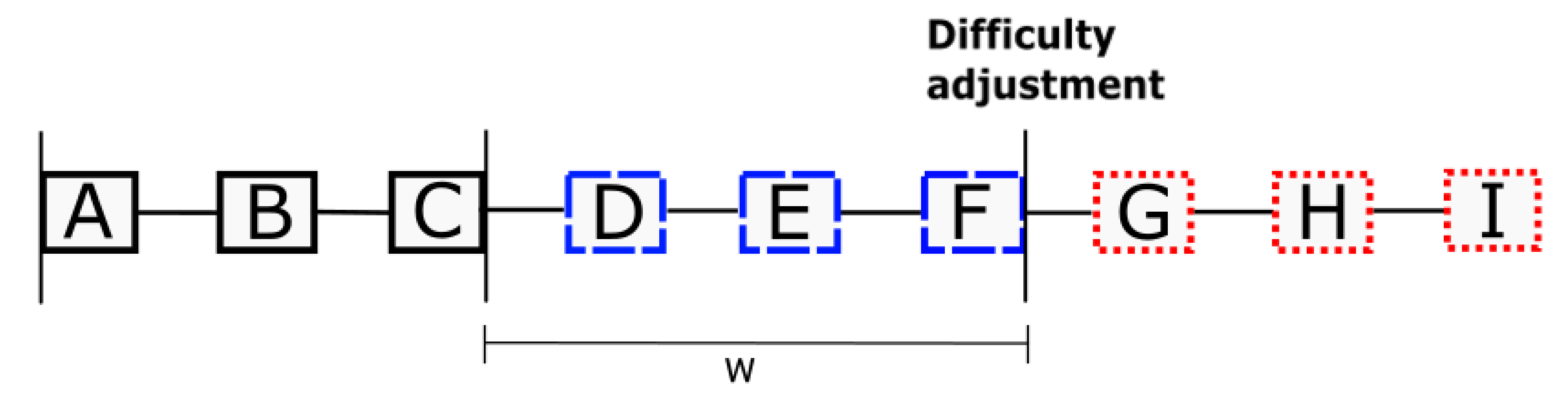
- Period-based
- Incrementally-extrapolated
- Sliding-window



Bitcoin: $w = 2016$

1. Period-based

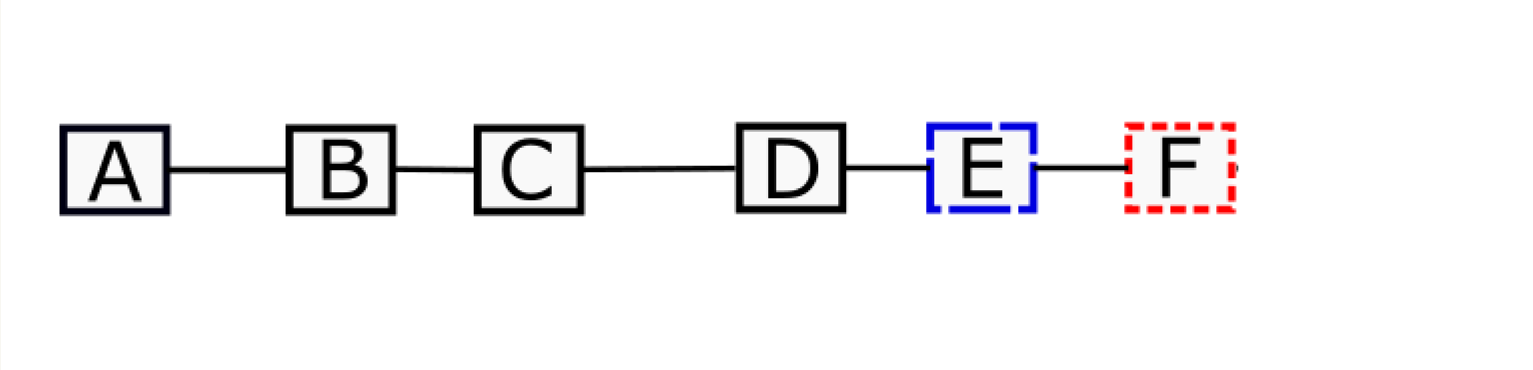
- Period-based
- Incrementally-extrapolated
- Sliding-window



$$\text{Bitcoin: } \tau_p = \frac{\left(\tau_{p-1} * (F_{time} - D_{time})\right)}{(\tau_{exp.} * w)}$$

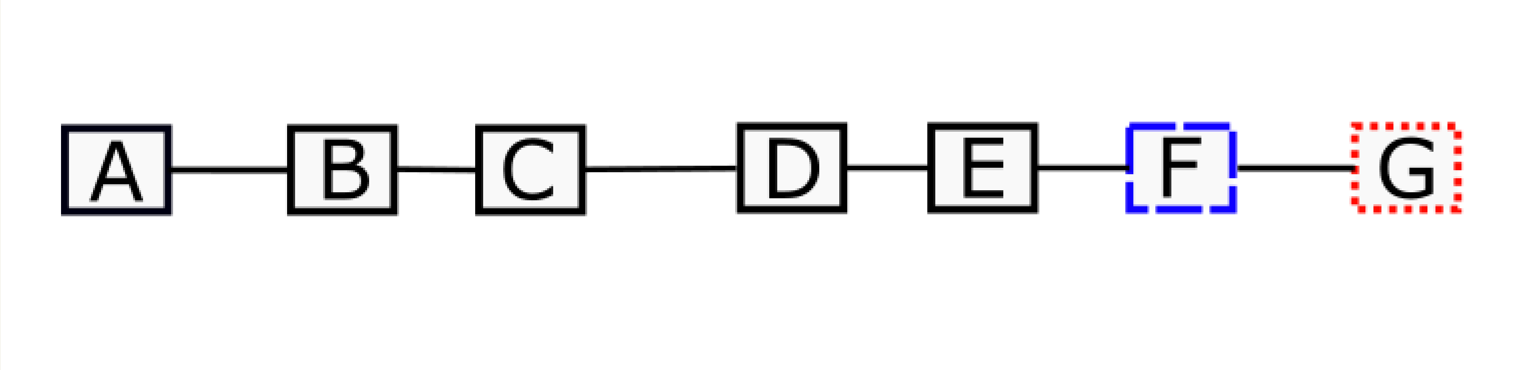
2. Incrementally-extrapolated

- Period-based
- Incrementally-extrapolated
- Sliding-window



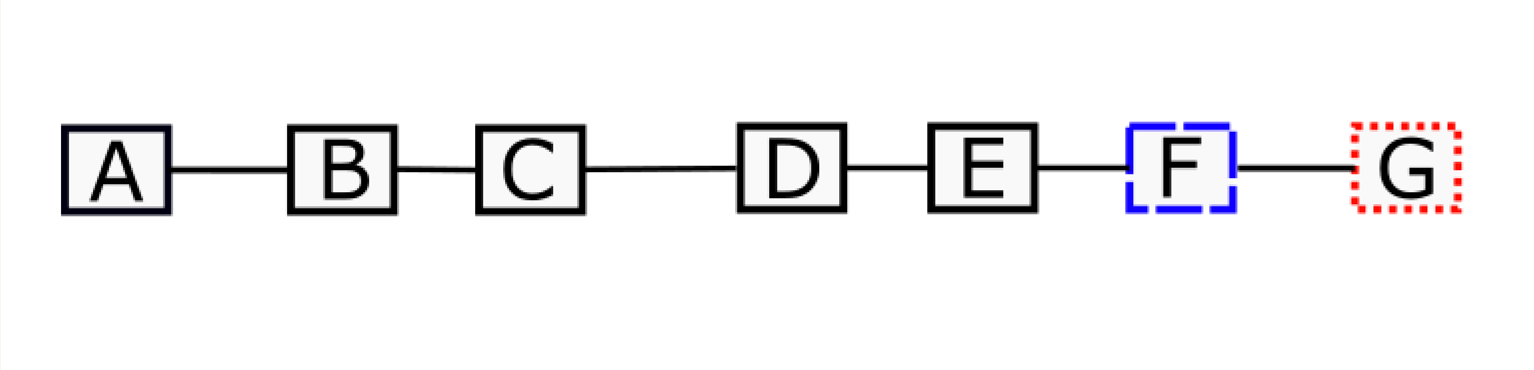
2. Incrementally-extrapolated

- Period-based
- Incrementally-extrapolated
- Sliding-window



2. Incrementally-extrapolated

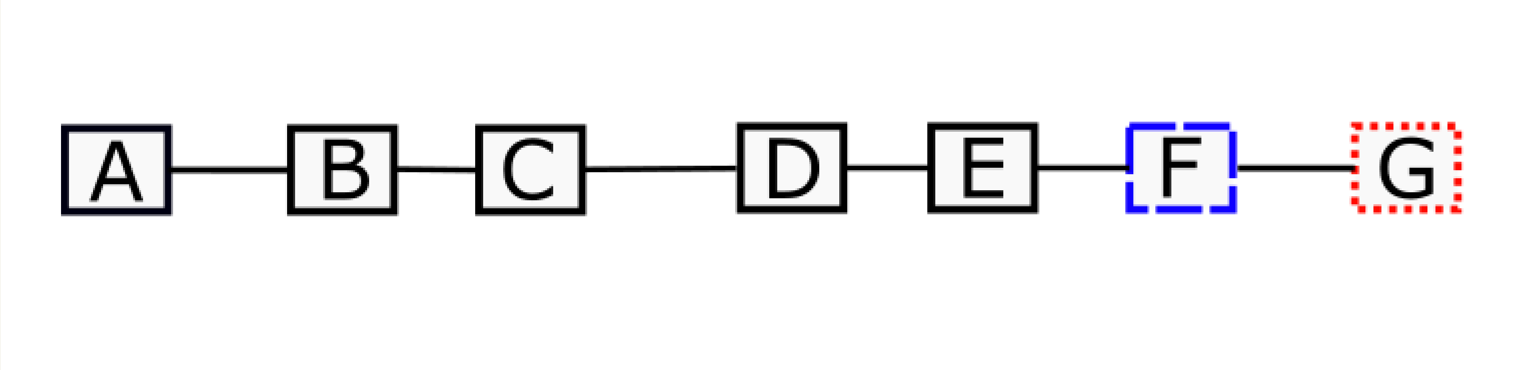
- Period-based
- Incrementally-extrapolated
- Sliding-window



Ethereum: $\tau_G = \tau_F + \left(\frac{\tau_F}{2048} * \left(1 - \frac{G_{time} - F_{time}}{9}\right)\right)$

2. Incrementally-extrapolated

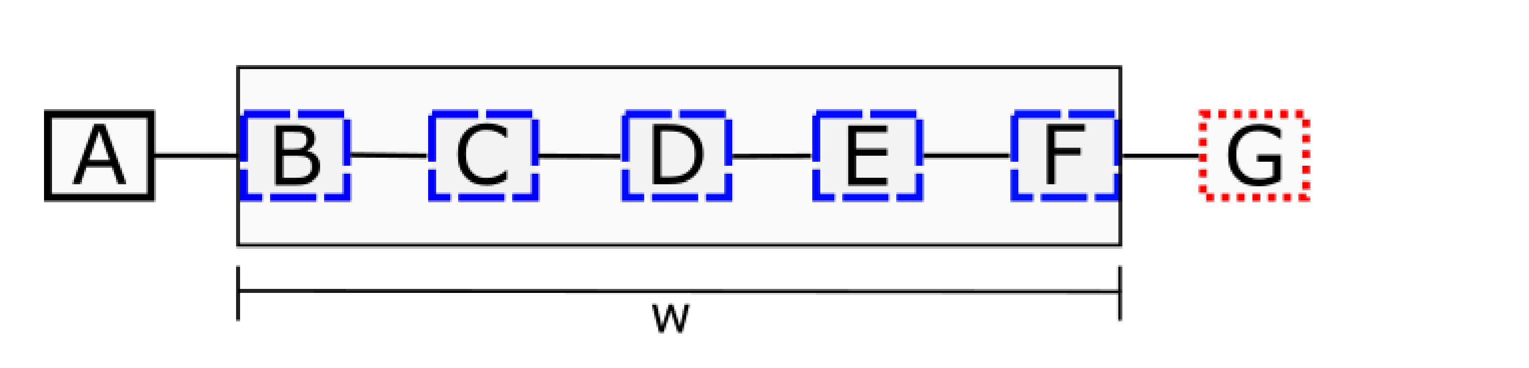
- Period-based
- Incrementally-extrapolated
- Sliding-window



Ethereum: $\tau_G = \tau_F + \underbrace{\left(\frac{\tau_F}{2048} * \left(1 - \frac{G_{time} - F_{time}}{9}\right)\right)}_{\text{Adjustment factor}}$

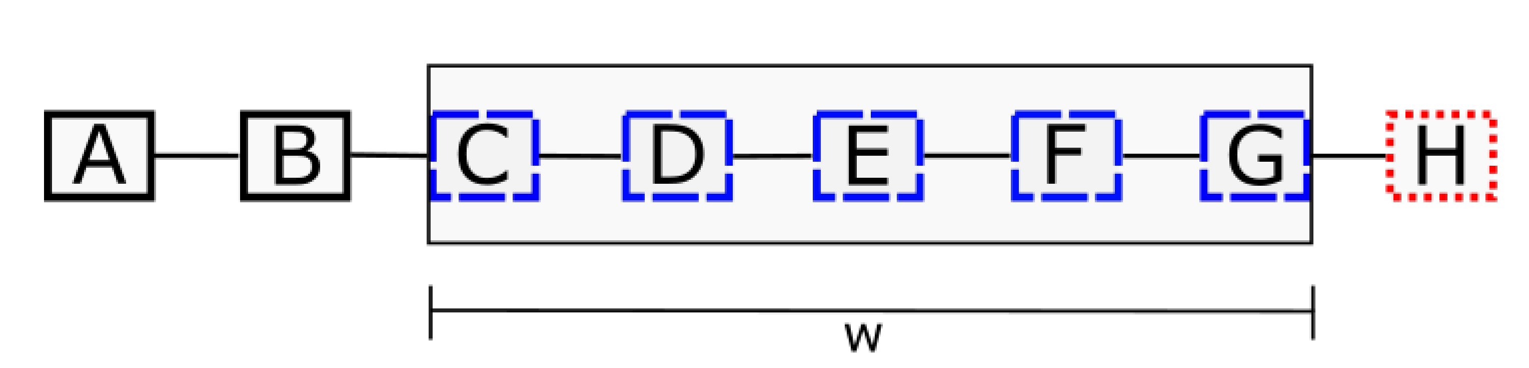
3. Sliding-window

- Period-based
- Incrementally-extrapolated
- Sliding-window



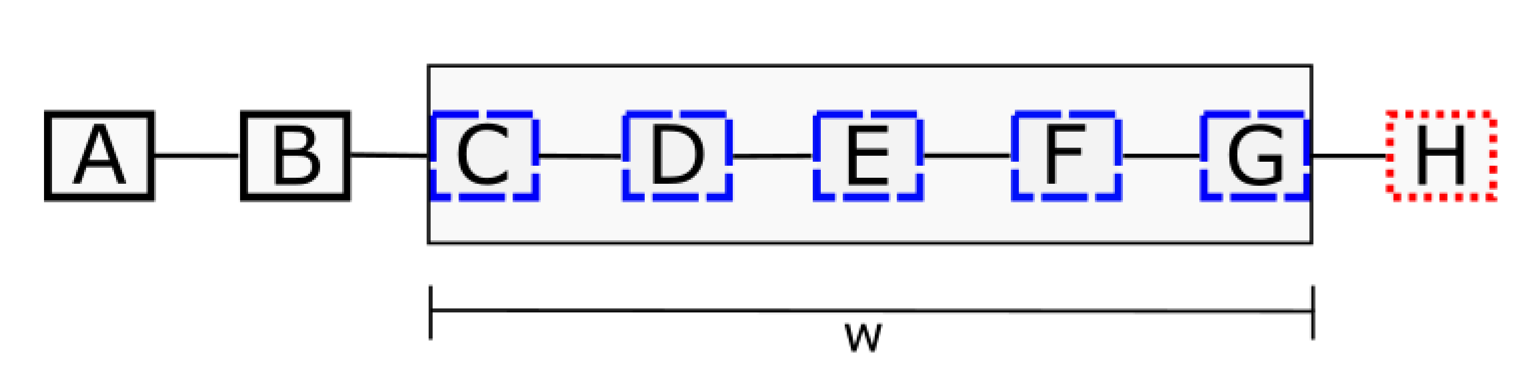
3. Sliding-window

- Period-based
- Incrementally-extrapolated
- Sliding-window



3. Sliding-window

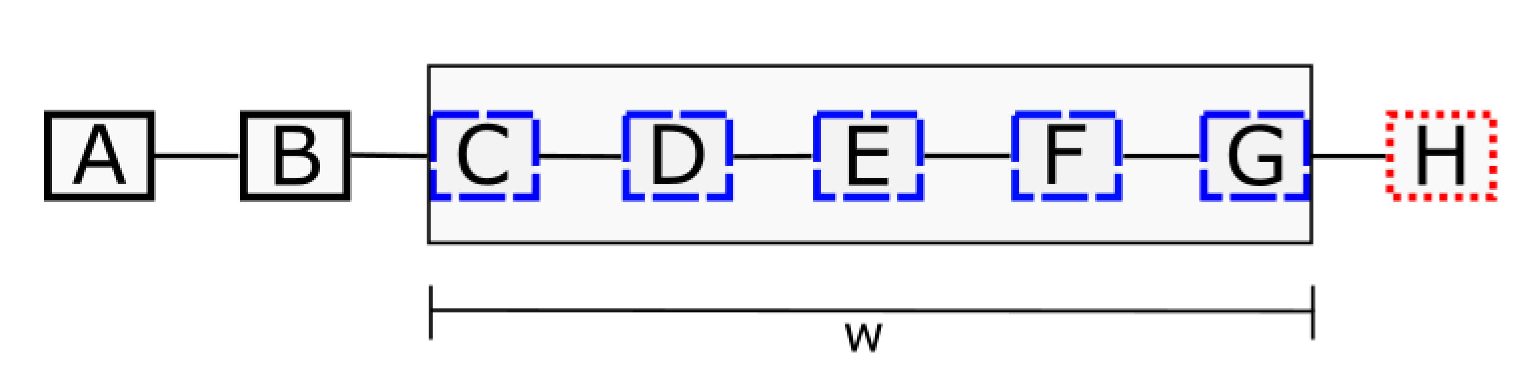
- Period-based
- Incrementally-extrapolated
- Sliding-window



BSV/BCH: $w = 144$ XMR: $w = 600$

3. Sliding-window

- Period-based
- Incrementally-extrapolated
- Sliding-window



BSV/BCH: $\frac{\left(\sum_{i=n}^{n+w} \tau_i\right)}{G_{time} - C_{time}}$

XMR: $\frac{\left(\sum_{i=n}^{n+w} \tau_i\right) * 120 + (G_{time} - C_{time}) - 1}{G_{time} - C_{time}}$

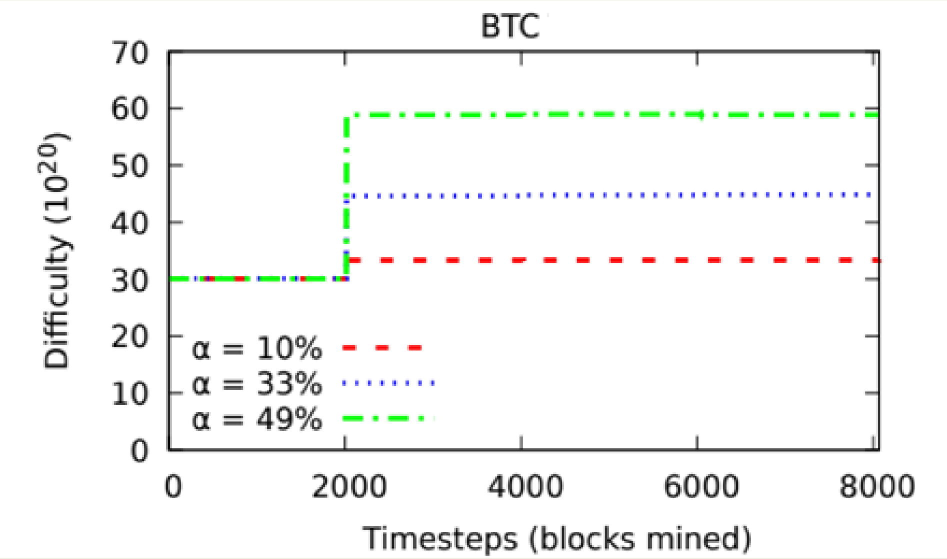
Evaluation

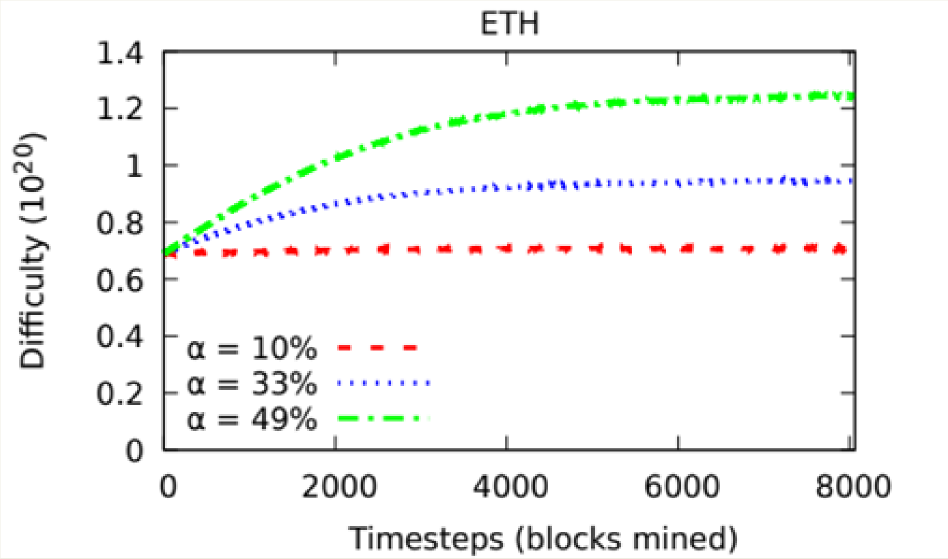
- How effective are DAAs at adjusting difficulty if a substantial amount of hash power is introduced to the network?

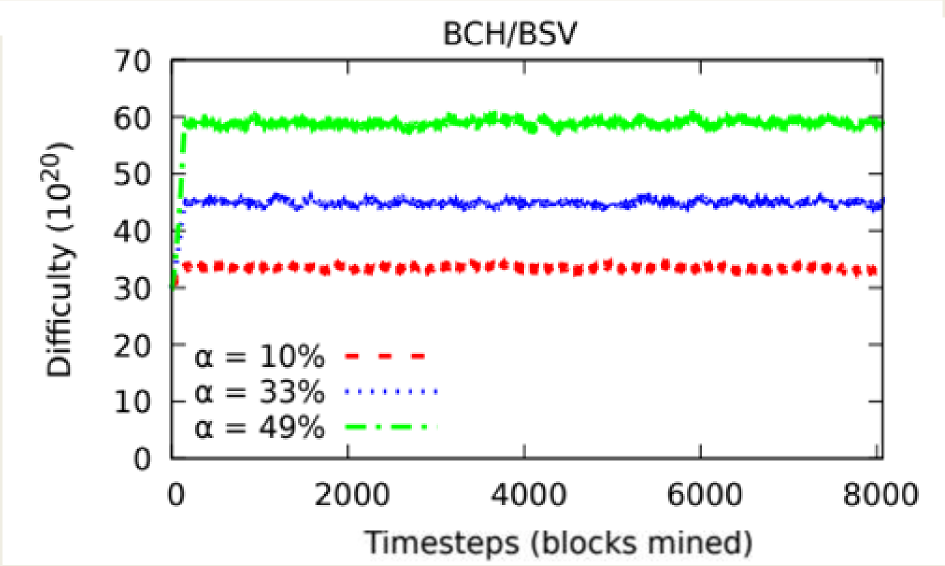
- How does difficulty affect the block win-rate of a new miner?

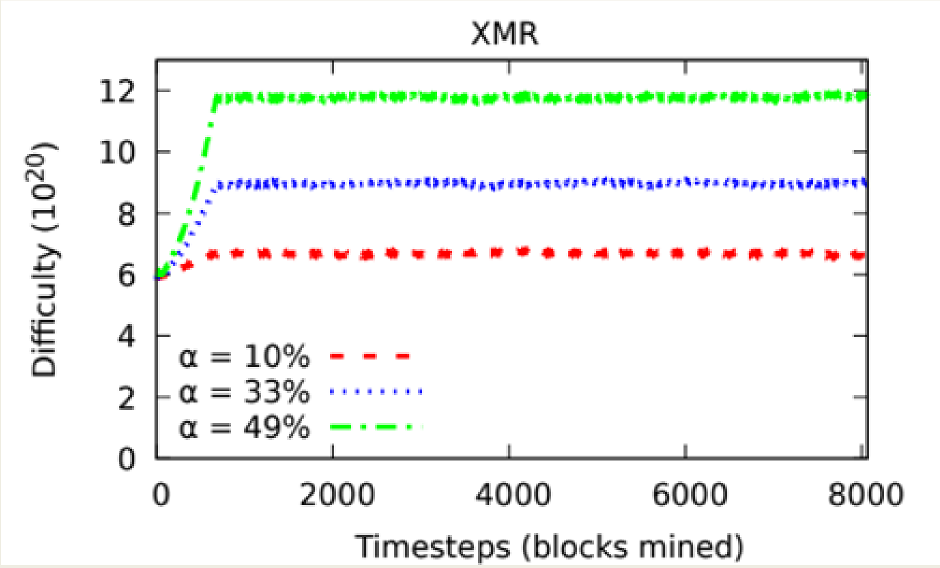
- How do these DAAs react to a new selfish miner?

Difficulty adjustment with a new honest miner

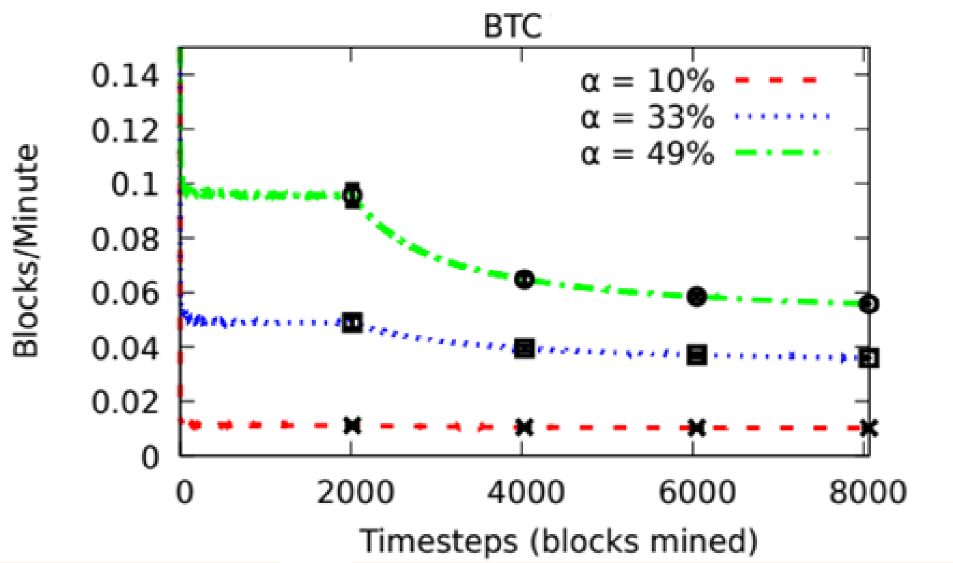


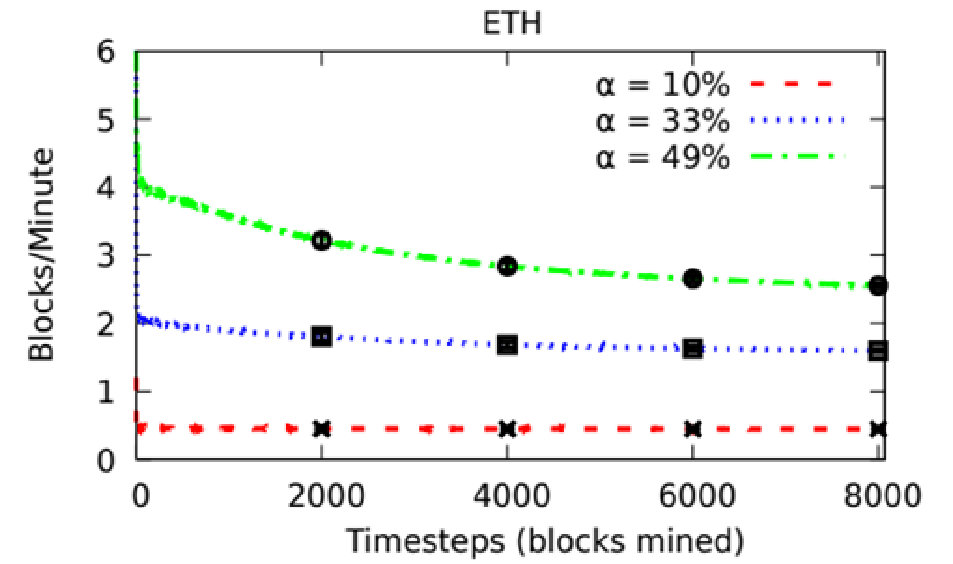


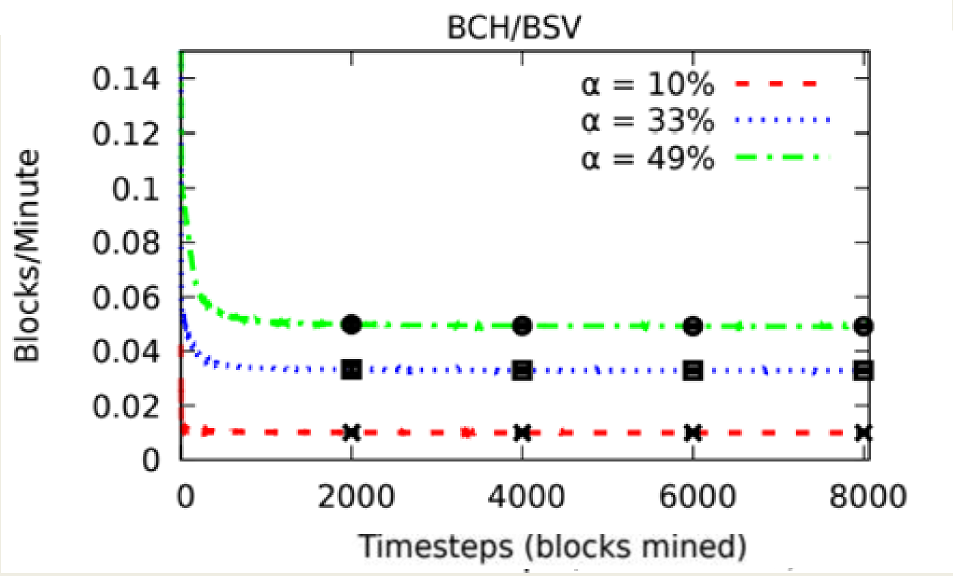


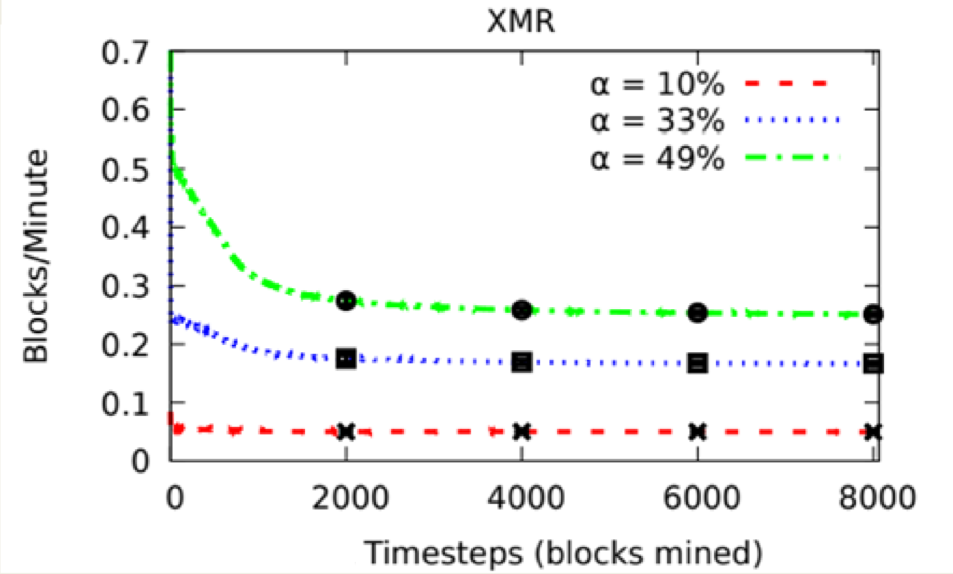


Block win-rate of a new honest miner

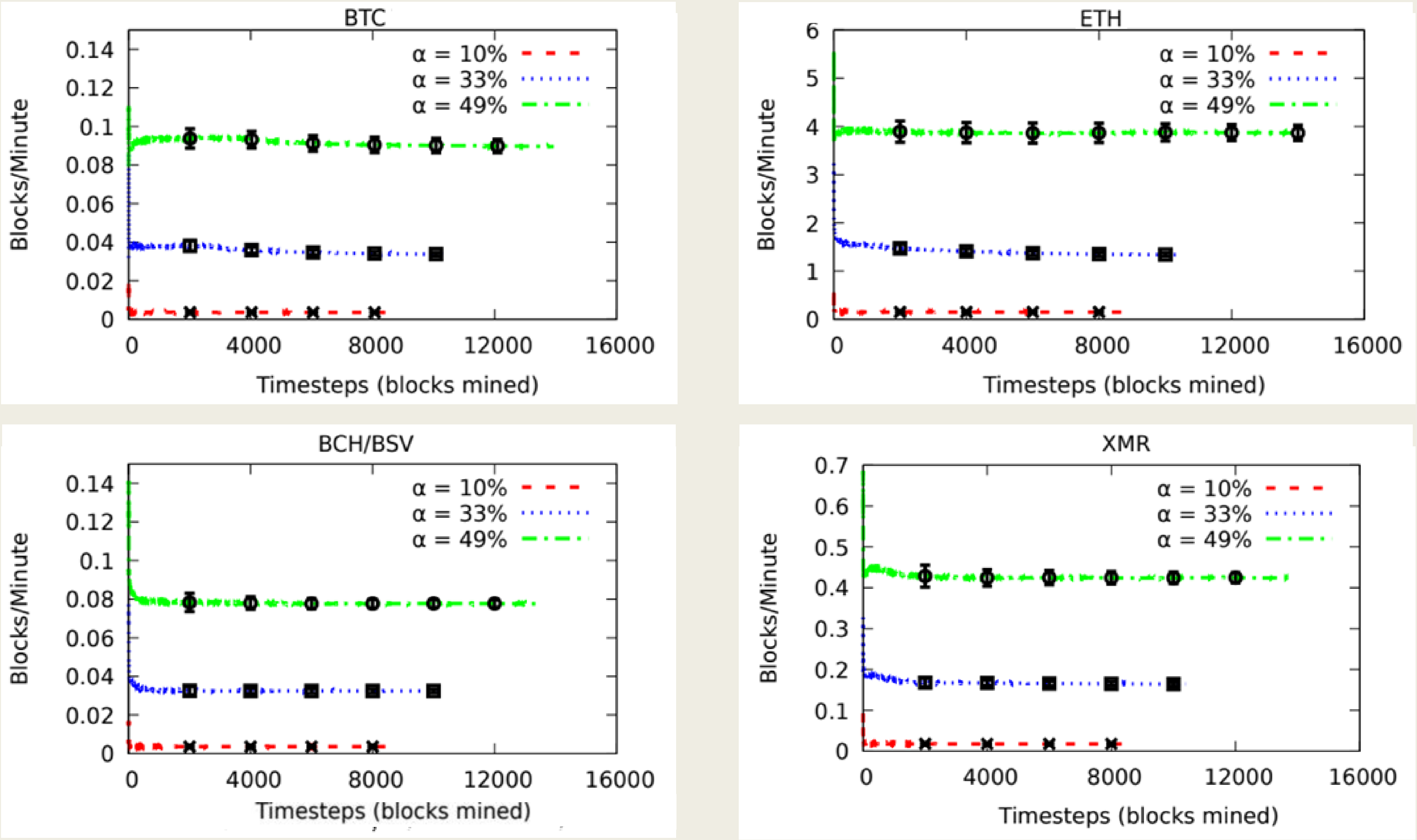




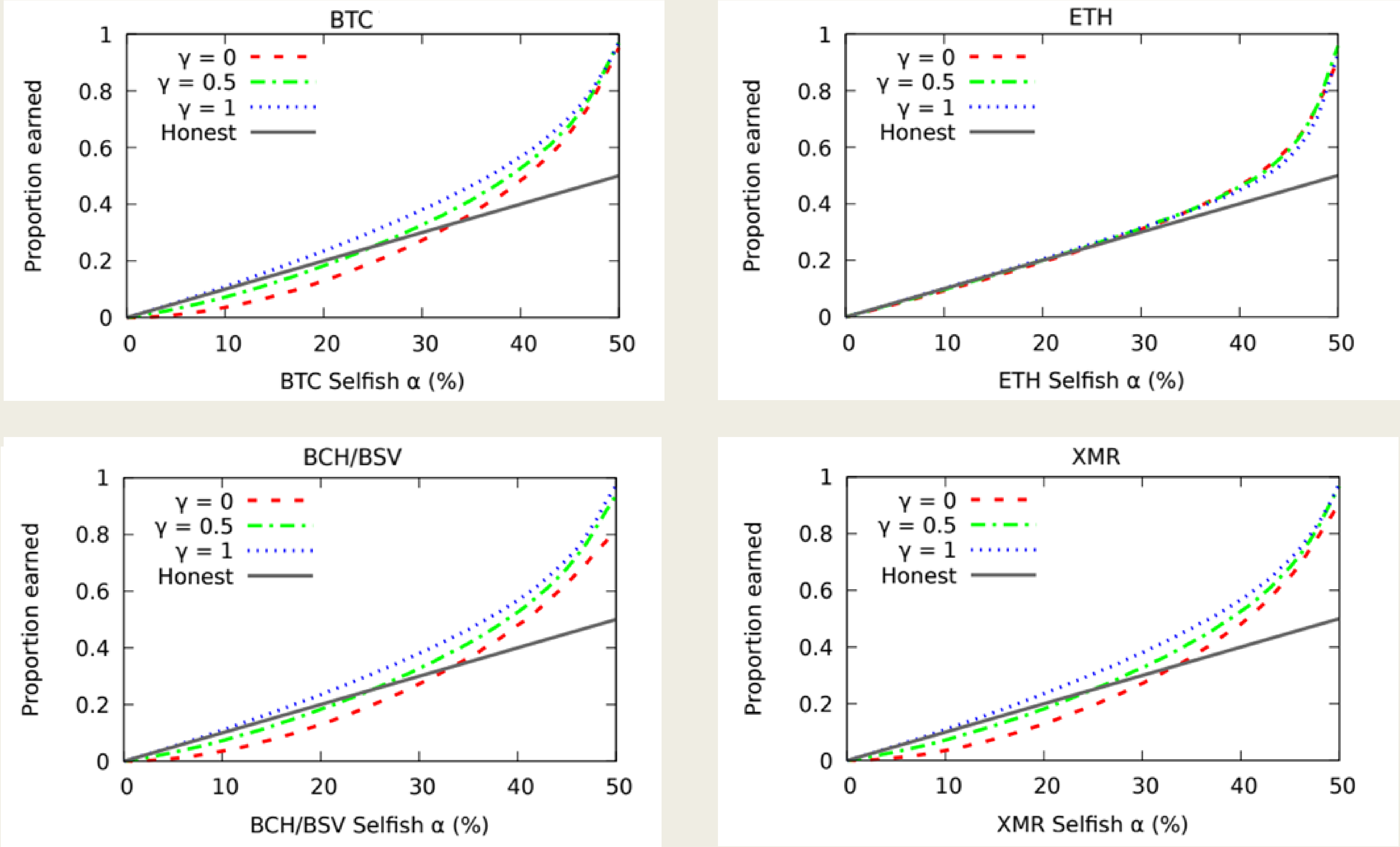




Block win-rate of a new selfish miner



Relative revenue of a new selfish miner



Findings

- Selfish mining does not need to persist past a difficulty adjustment to be profitable
- Above a threshold, selfish mining is profitable per time-unit regardless of DAA choice
- The choice of DAAs can exacerbate the selfish mining threat
- Ethereum is vulnerable due to uncle block rewards

Summary

- Introduced novel intermittent selfish mining strategy
- Provided a taxonomy for difficulty adjustment algorithms
- Analyzed the profitability of selfish mining with various DAAs

Whither selfish mining?

- Deviant miners do not self-report
- Miners have stake in the system and after-effects are unknown
- Miners may lack know-how to implement selfish mining
- For popular cryptocurrencies, the hash power required is too expensive for a single adversary to acquire

Gamma values

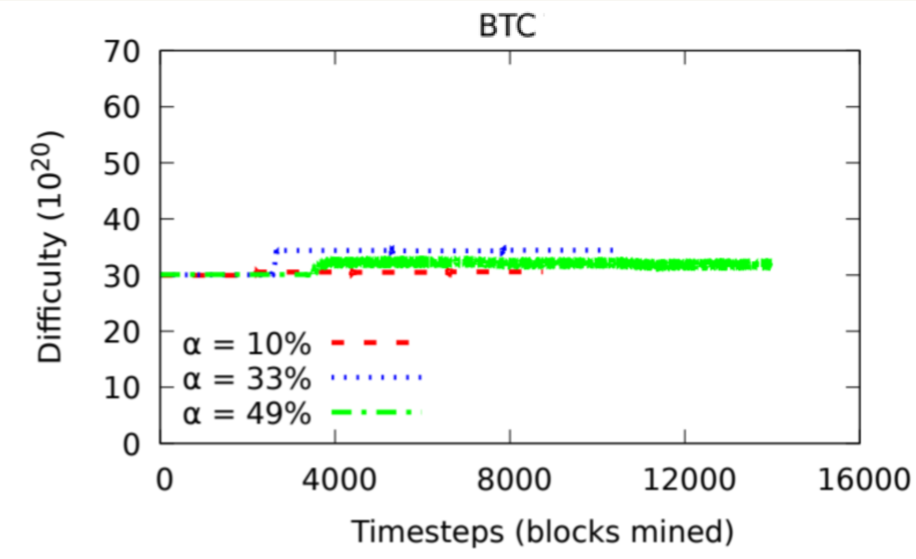
- γ : proportion of honest miners who mine on the selfish block in a fork

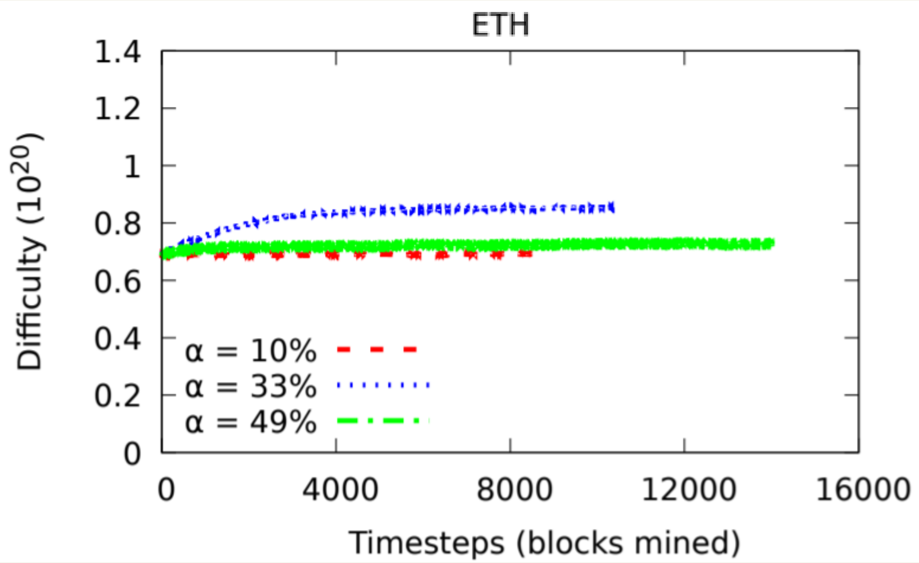
- $\gamma = 1$: selfish miner wins all forks

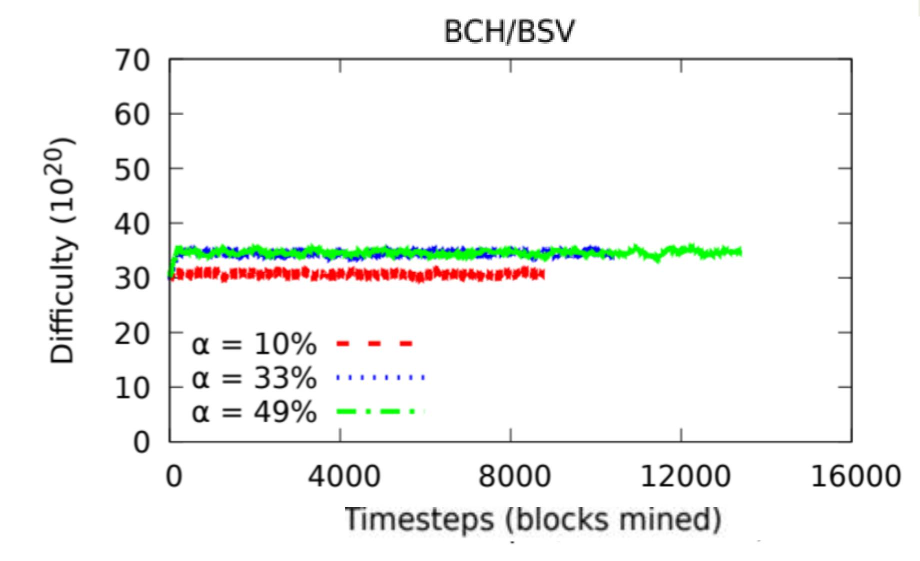
- $\gamma = 0$: selfish miner loses all forks

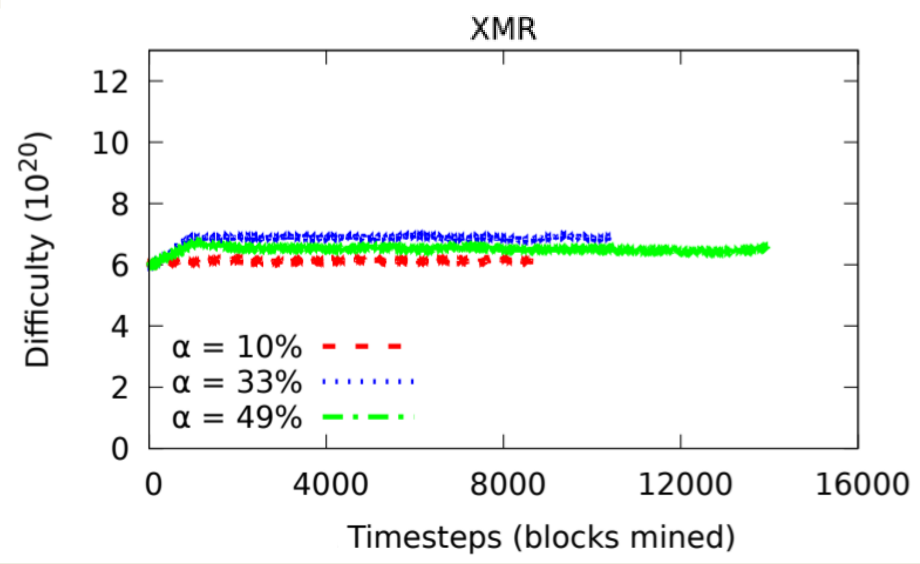
- $\gamma < 0$: nonsense

Difficulty adjustment with a new selfish miner

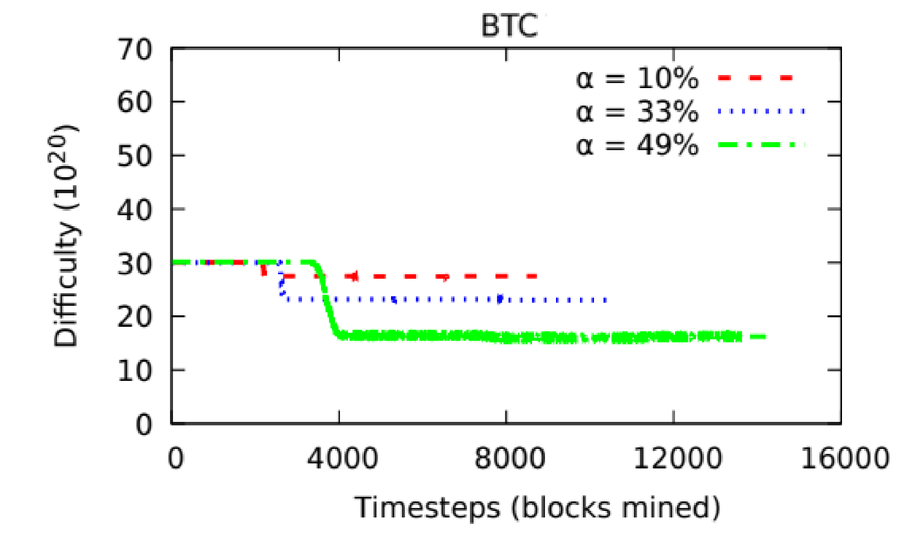


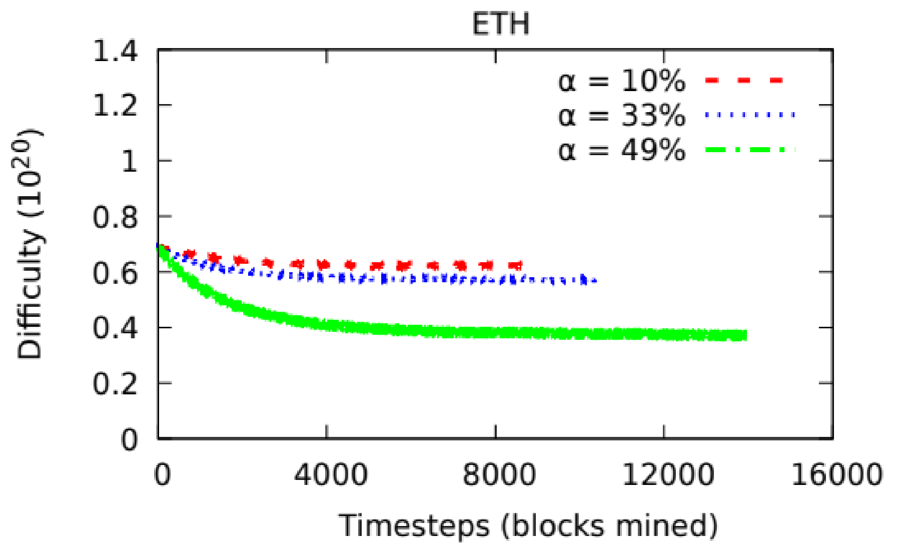


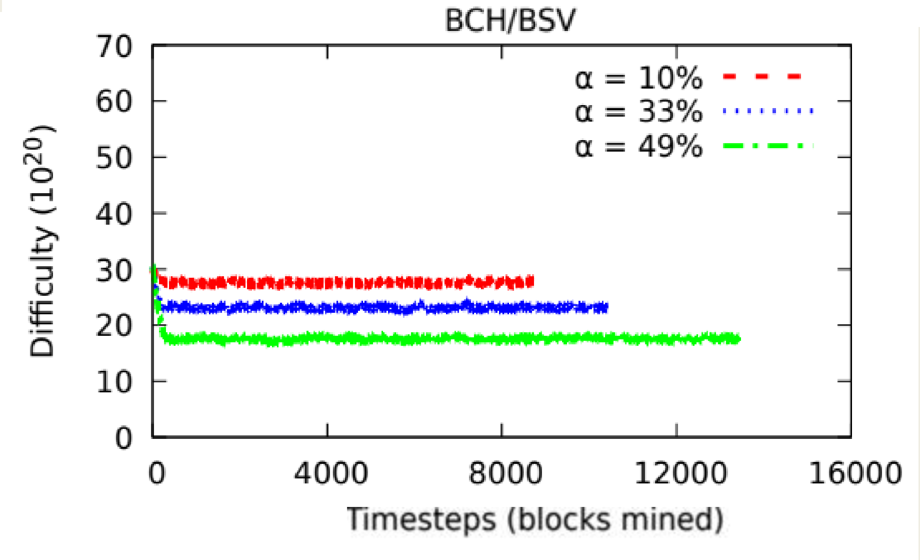


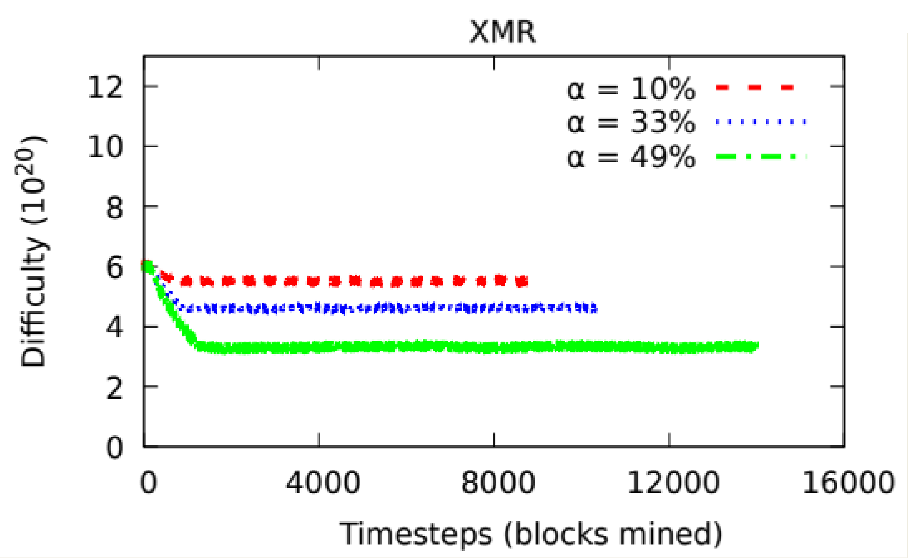


Difficulty adjustment with an existing selfish miner

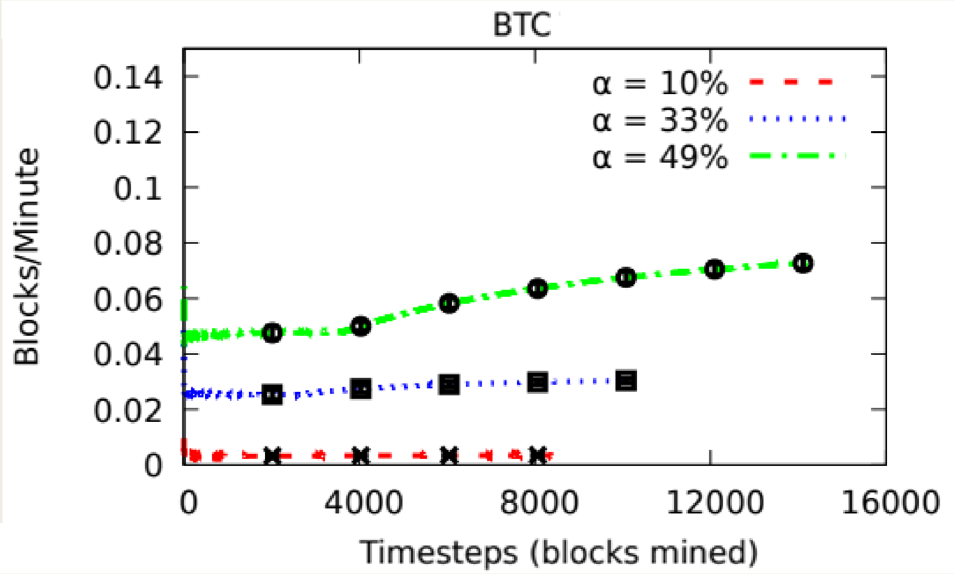


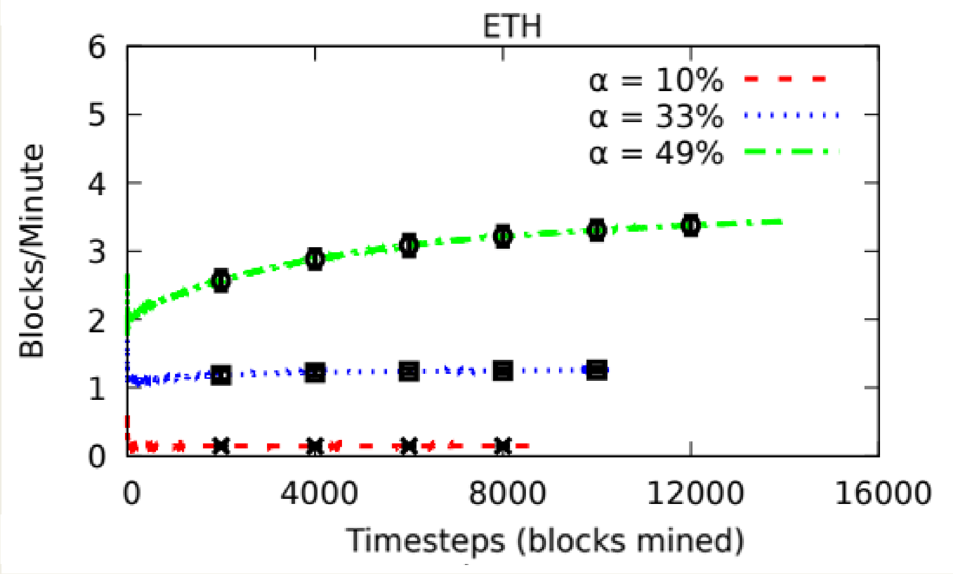


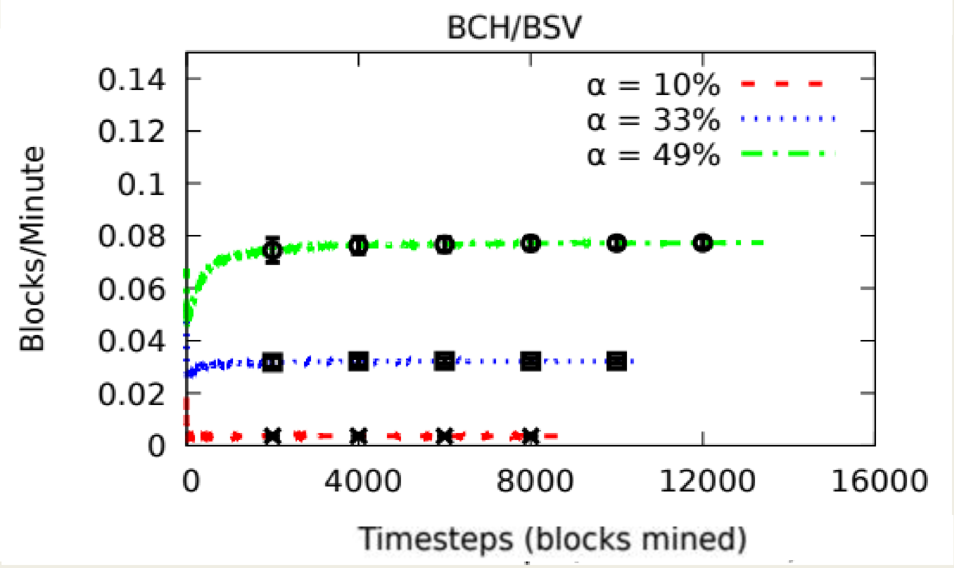


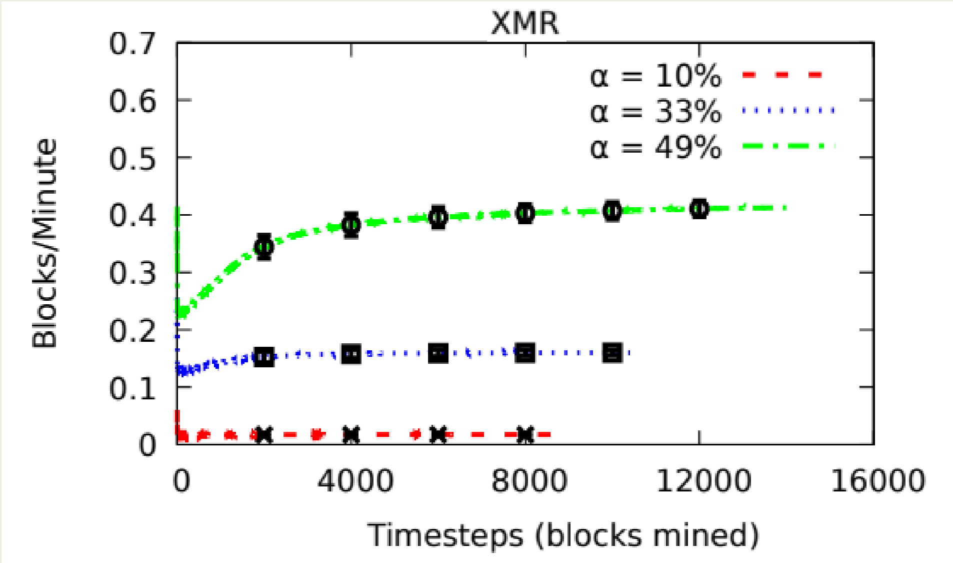


Block win-rate of an existing selfish miner

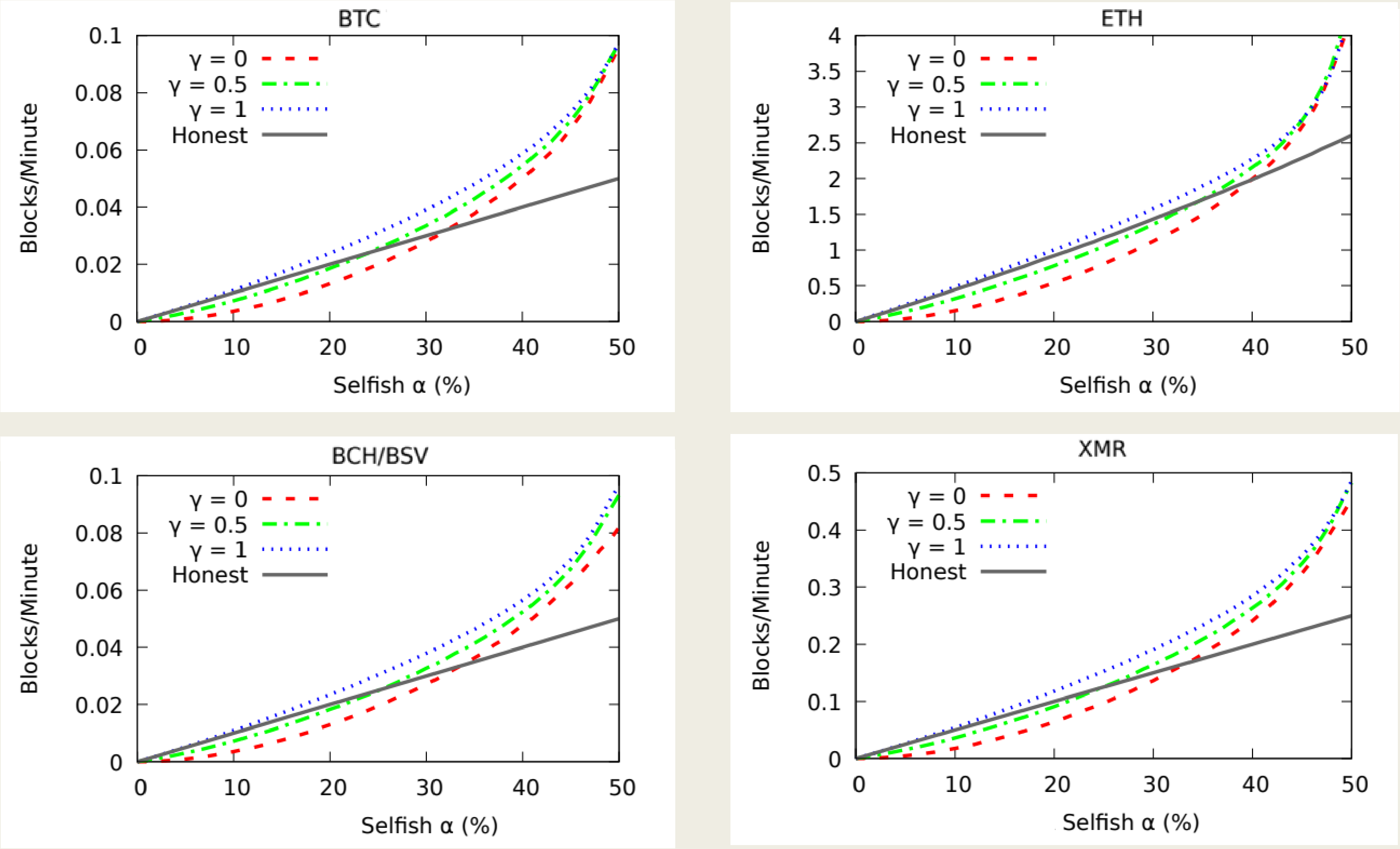








Block win-rate of an existing selfish miner


BTC
ETH
BCH/BSV
XMR
γ = 0
γ = 0.5
γ = 1
Honest
Blocks/Minute
Selfish α (%)