Compounding of Wealth on Proof-of-Stake Cryptocurrencies

JAEWAN HONG

Proof of Stake

VIRTUAL MINING TO REPLACE COMPUTATIONAL PUZZLES

Why Virtual Mining?

- Power on meaningless computation

Why Virtual Mining?

- Power on meaningless computation

- ✓ Fast?
- ✓ Efficient?
- ✓ Platform?
- ✓ Functions?
- ✓ Applicable?

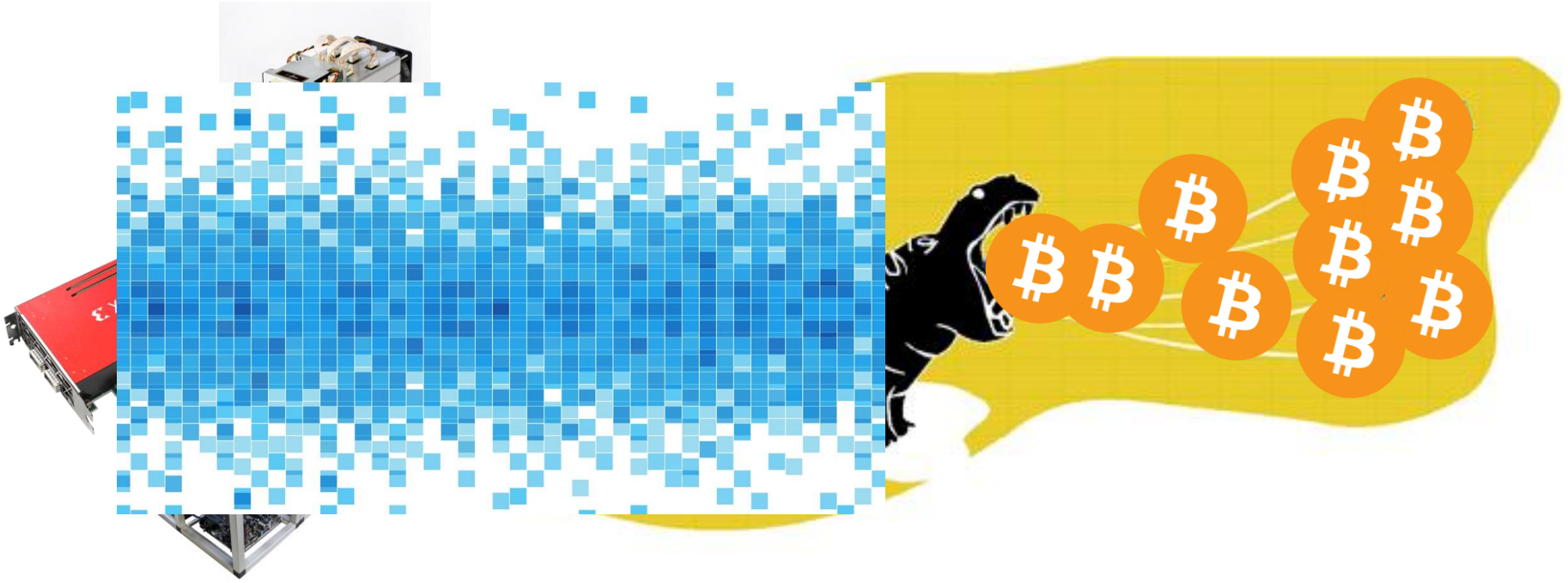
Why Virtual Mining?

- Power on meaningless computation

- ~~Fast?~~
- ~~Efficient?~~
- ~~Platform?~~
- ~~Functions?~~

Why Virtual Mining?

- Power on meaningless computation

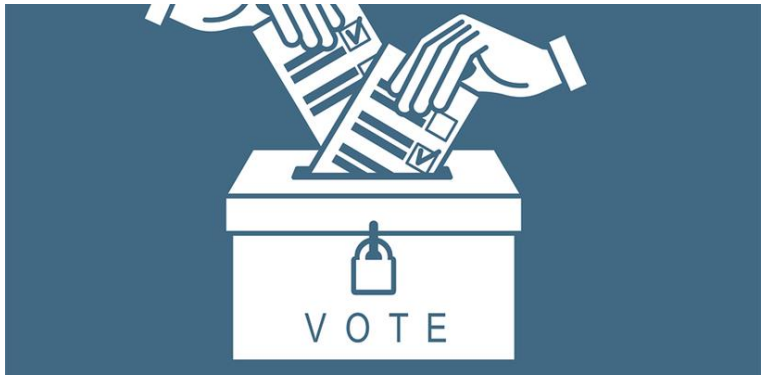


- ~~Fast?~~
- ~~Efficient?~~
- ~~Platform?~~
- ~~Functions?~~

Why Mining?

- Which Block to Append?

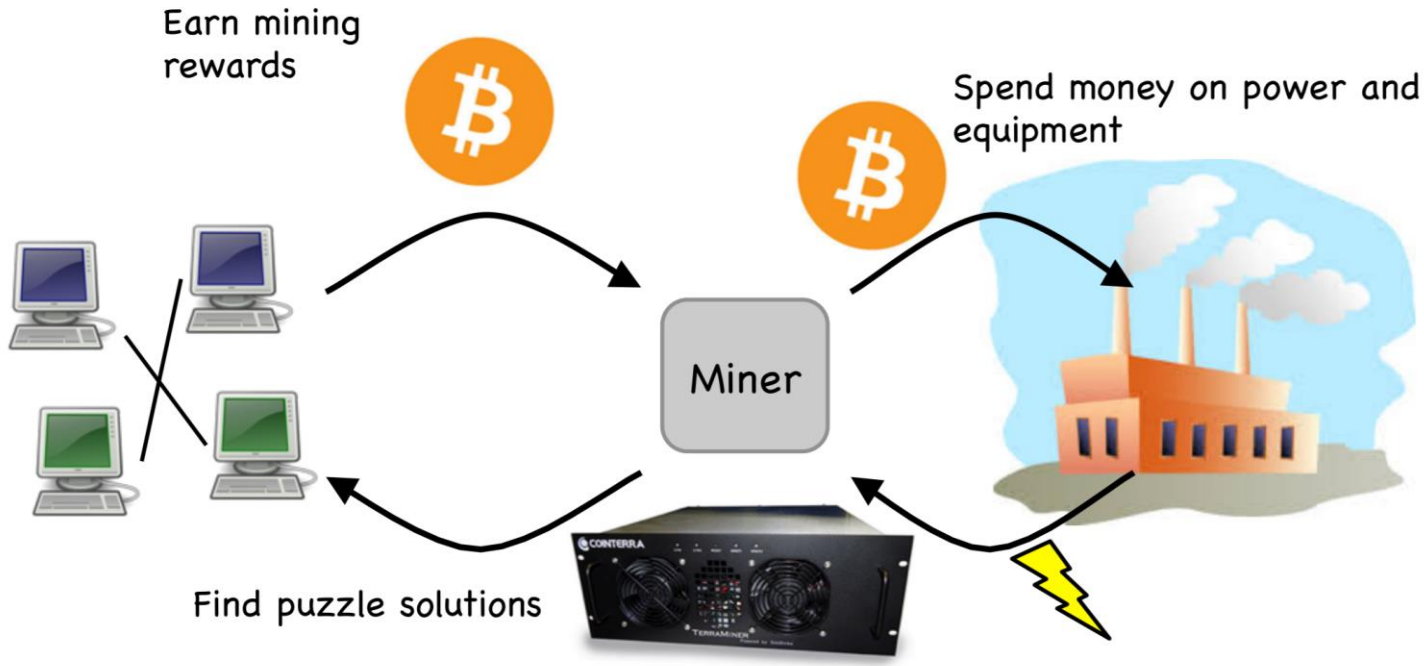
- Select a leader to propose the next block



- Leader Proposes a block

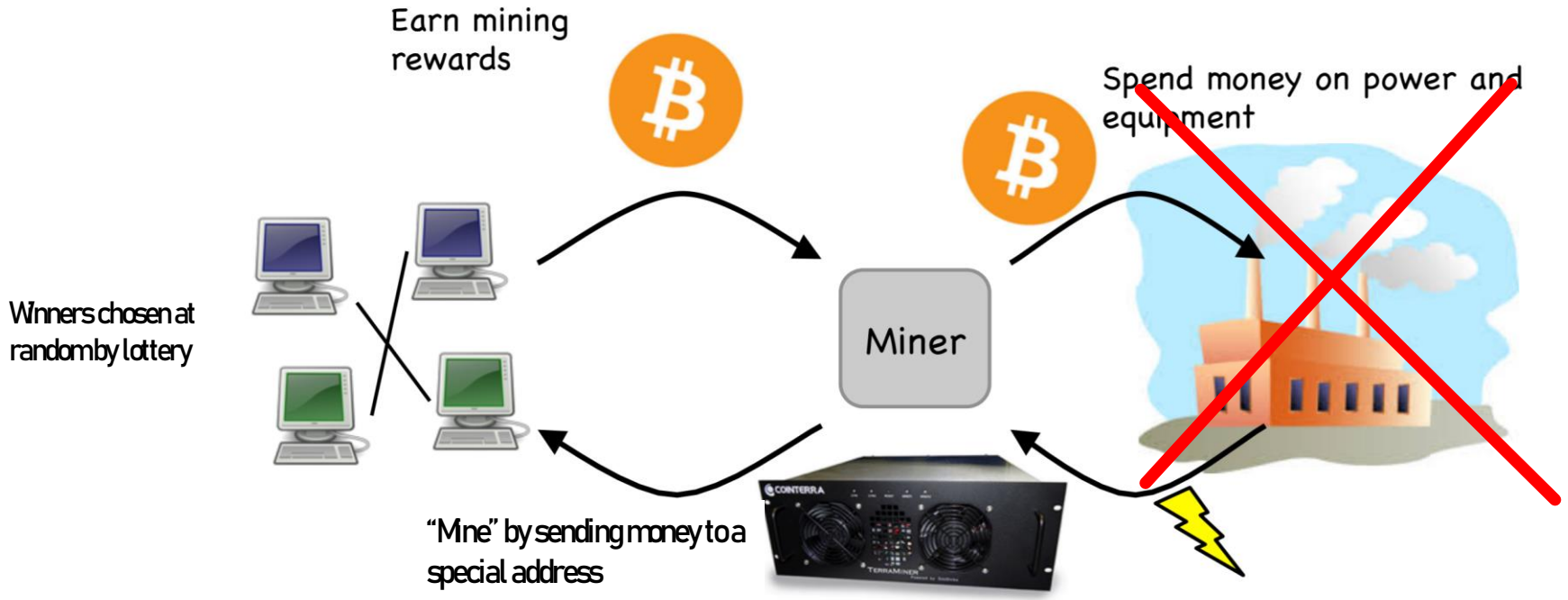
Underlying Questions on PoW

- What would happen if we removed the step of spending money on power and equipment?



Underlying Questions on PoW

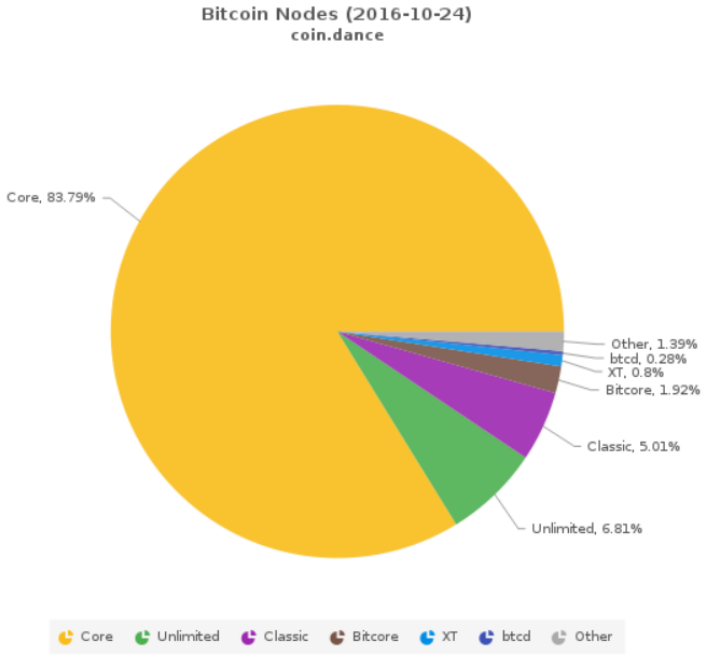
- Why not simply allocate mining power directly to all currency holders in proportion to how much currency they actually hold?



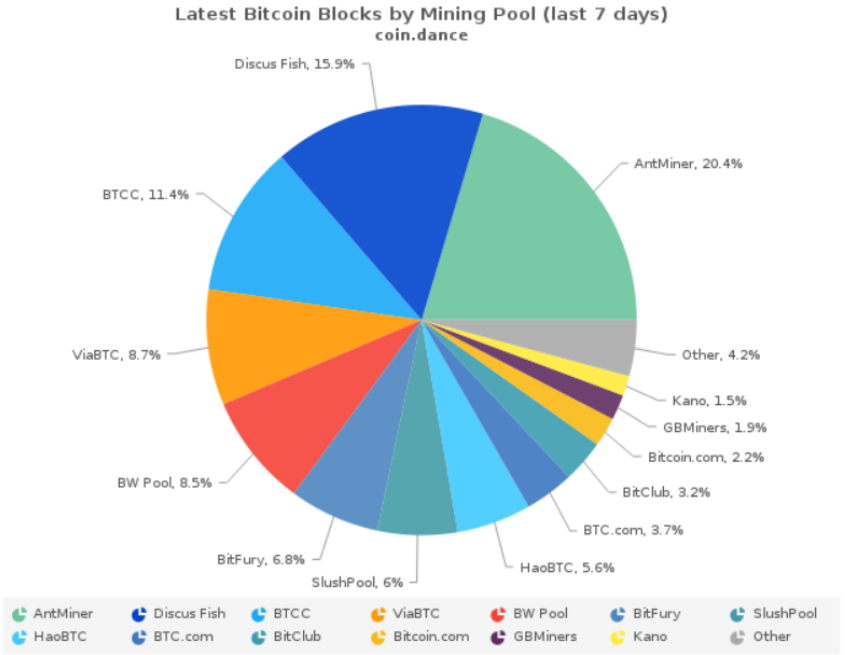
- ✓ Election, transaction verification
- ✓ Scaling

Why PoS?

- May also reduce the trend toward centralization. Satoshi Spirits



Client Centralization



Mining Centralization

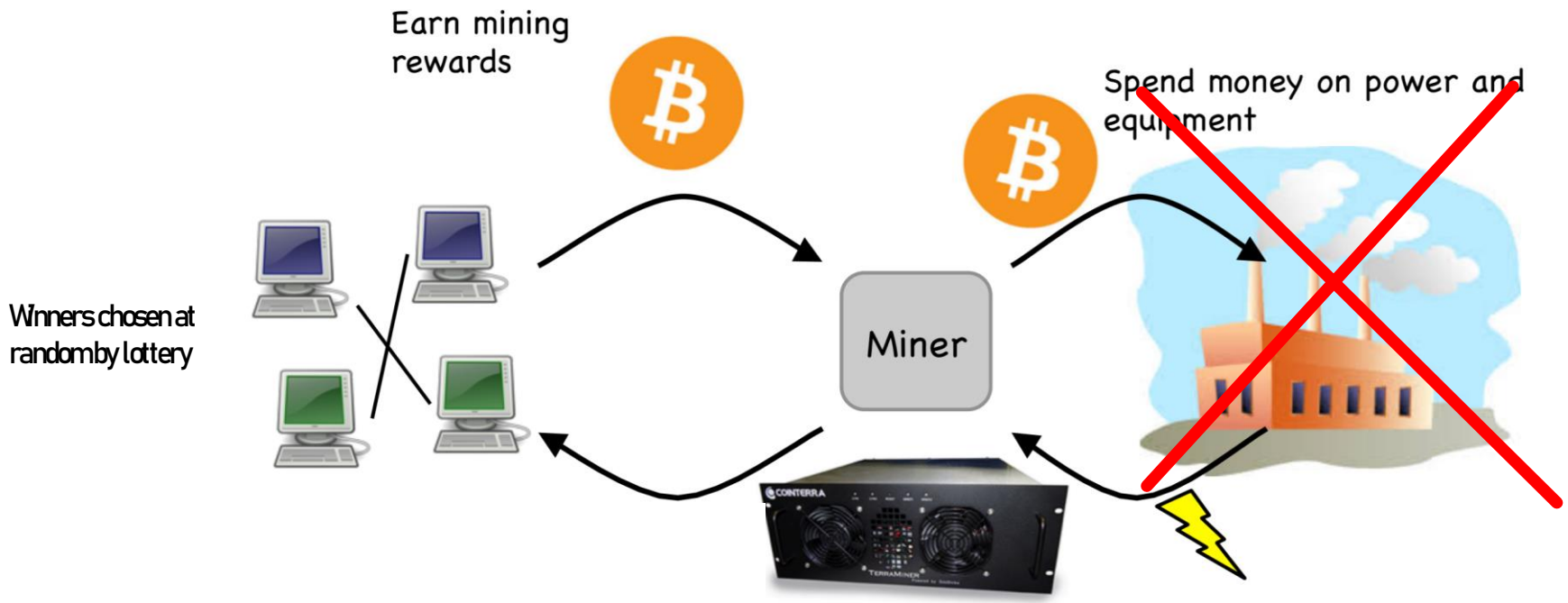
Why PoS?

Asic Resistance

Better Stewards

Understanding PoS

- How does lottery work?



Understanding PoS

- General Case

Random Seed

Understanding PoS

- Each miners run the lottery machine

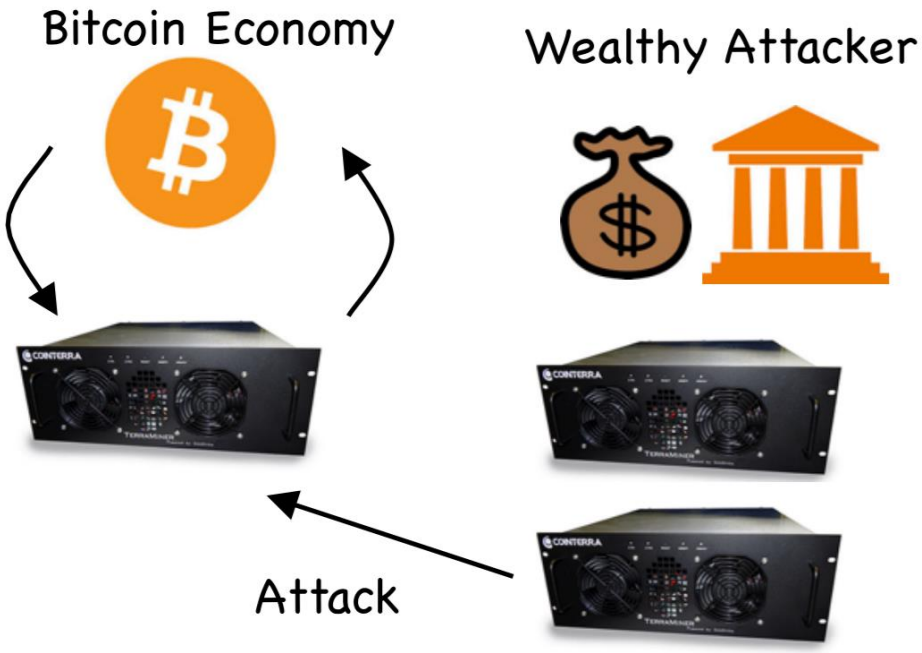
Stake Fraction

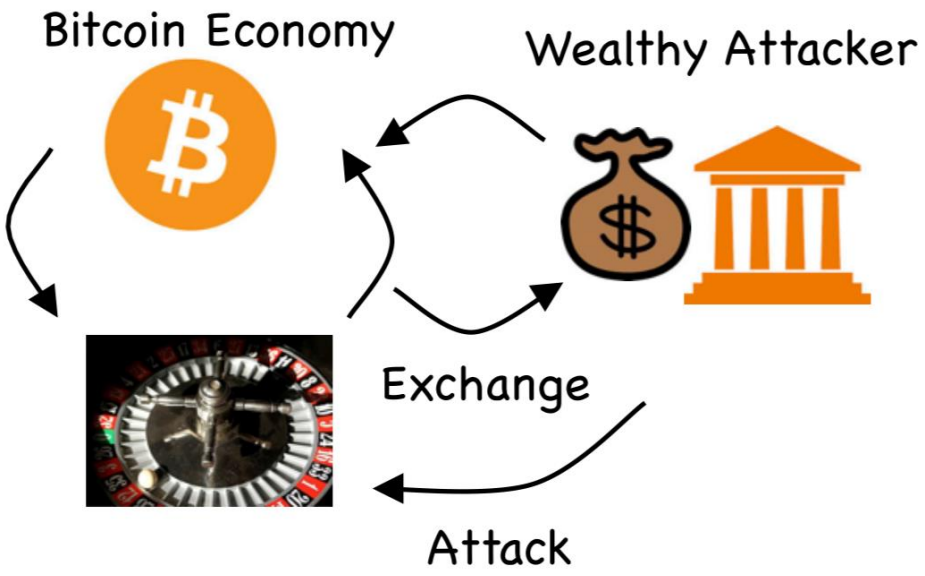
Random Seed

=Res smallest or closest to a value is elected

51% Attack Prevention

- Votes determined by how much currency one currently holds instead of mining power





Problems of PoS

- Rich get Richer
  - Purest form of PoS makes mining easier for those who can show they control a large amount of currency
  - The richest participants are always given the easiest mining puzzle.
- Attacks
  - Grinding attack
  - Desynchronization attack
  - Eclipse Attack
  - Bribery Attack
  - Network Splitting

Nothing-at-Stake Problem

- Nothing-at-stake problem or stake-grinding attacks
- An attacker with a proportion a<0.5 of the stake is attempting to create a fork of k blocks
  - In PoW, a failed attack has a significant opportunity cost
  - Virtual mining, this opportunity cost doesn't exist.
- Virtual mining can use his stake to mine in the current longest chain while simultaneously attempting to create a fork
  - Thus, rational miners might constantly attempt to fork the chain

Alternate Forms of Stake

- Proof of Deposit
  - When coins are used by a miner to mint a block, they become frozen for a set number of blocks
  - System rewards miners who are willing to keep coins unspent for a long time into the future
  - Miners' stake effectively comes from the opportunity cost of not being able to use the coins to perform other actions
  - Claim a coin after some time
- Proof of Burn
  - Mining with a coin destroys it
- Proof of Activity
  - Any coin might be win (if online)

Algorand Election Policy

- Every user runs its own ‘lottery machine’(VRF) fueled with a public random seed and its private key
- Produce uniformly distributed random values
- If the value of the ticket is close to some target value, then participate in proposing or validating blocks
- Chance proportional to the fraction of stake

Cardano Election Policy

- Follow-the-Satoshi algorithm takes a random seed from previous round
- One round is divided into slots
- Choose the minimum stake holders slot leaders
- Slot leaders propose a block

Dfinity Election Policy

- Proposer elected upon the random seed from previous round
- Every round starts with an update of the registered users
- Pseudo-random permutation on all users and ranks all block proposals through random seed
- Deposited money confiscated if misbehave

Peercoin Election Policy

- Hybrid of PoW/PoS in which stake is denominated by "coin-age"
- The coin-age of a specific unspent transaction output is the product of the amount held by that output and the numbers of blocks that output has remained unspent
- To mine a block, solve SHA-256 but the difficulty is adjusted down by coin-age miners consume

Too Many Candidates

	Algorand	Cardano	Dfinity	Snow White
Primitive	VRF	Coin-Tossing PRF	VRF (Threshold Signature)	Coin-Tossing PRF
Elect Block Proposers	Yes	Yes	Yes	Yes
Validating Committee	1000 (flexible)	No	1000 (flexible)	No
Stake weighted	Yes	Yes	Deposit-based	Yes (without Specification)
Consensus	BA* (Instant Finality)	Nakamoto Style	Chain "weight" + Notarization	Nakamoto Style

Too Many Candidates

Compounding of Wealth in PoS Cryptocurrencies

Giulia Fanti et al. FC19
(Slides Based on Archive full Version)

Towards a Unified Metric for Performance Evaluation of Proof-of-Stake Blockchains

Sergey Gorbunov Follow
May 25, 2018 · 5 min read

Sergey Gorbunov and Silvio Micali

Blockchain systems need to scale to process thousands of transactions per second, while remaining decentralized and secure against powerful attack vectors. However, decentralization, security and performance always play a 3-way tug of war and trade-offs between these properties are typically made. These properties are the core pillars of a blockchain system! Simultaneously achieving high-degrees of all three properties for any system is very challenging.

Common Metric Needed

One of the problems we see with the ecosystem is a lack of a common framework for analyzing performance of blockchain systems. Different projects rely on totally different measures, making meaningful comparison essentially impossible. Often hundreds, thousands, or millions of transactions per second are claimed without clarifying the underlying assumptions or settings.

Main Contributions

Equitability

Metric to mathematically compare PoS, PoW, and other block reward schemes.

How much the fraction of total stake belonging to a node can grow or shrink

T_i, R_i variable

Guideline to choose r(n)

Geometric Reward Function

Rewards increase geometrically

Unique solution to an optimization problem on the second moment of a time-varying urn process

MO-k Strategy

Match-Override-k

Selfish mining strategy optimized for PoS

Strategic behavior

Equitability

Equitability in Expectation

- Desirable property
  - Fractional stake remain constant

$$\mathbb{E}[v_{A,r}(n)] = v_A(0)$$

V_A = Stake Fraction, r =reward

Equitability in Expectation

- Expected fractional stake is a straw-man metric

$$\mathbb{E}[v_{A,r}(n) \mid v_{A,r}(n-1) = v]$$
$$= v\frac{v\,S(n-1) + r(n-1)}{S(n)} + (1-v)\frac{v\,S(n-1)}{S(n)} = v$$

- All reward function yield the same expected fractional stake

Equitability in Variance

- Reward function can dramatically change the distribution of the final stake

- ⬇ variance == ⬇ uncertainty == ⬆ Equitability

$$\mathrm{Var}\left(v_{A_i,r_1}(T)\right) \leq \mathrm{Var}\left(v_{A_i,r_2}(T)\right)$$

- Reward function 1 is more equitable than reward function 2

Equitability in Variance

- Depends only on reward function r and the time T. No $V_A(0)$

$$Let\ e^{\theta_n} \triangleq S(n)/S(n-1),\ then$$

$$\mathrm{Var}(v_{A,r}(T)) = \left(v_{A,r}(0) - v_{A,r}(0)^2\right)\left(1 - \frac{S(0)^2}{S(T)^2}\prod_{n=1}^{T}(2e^{\theta_n} - 1)\right)$$

Equitability in Variance

- Depends only on reward function r and the time T. No $V_A(0)$

It is sufficient to consider a single party's stake

$$Let\ e^{\theta_n} \triangleq S(n)/S(n-1),\ then$$

$$\mathrm{Var}(v_{A,r}(T)) = \left(v_{A,r}(0) - v_{A,r}(0)^2\right)\left(1 - \frac{S(0)^2}{S(T)^2}\prod_{n=1}^{T}(2e^{\theta_n} - 1)\right)$$

Equitability in Variance

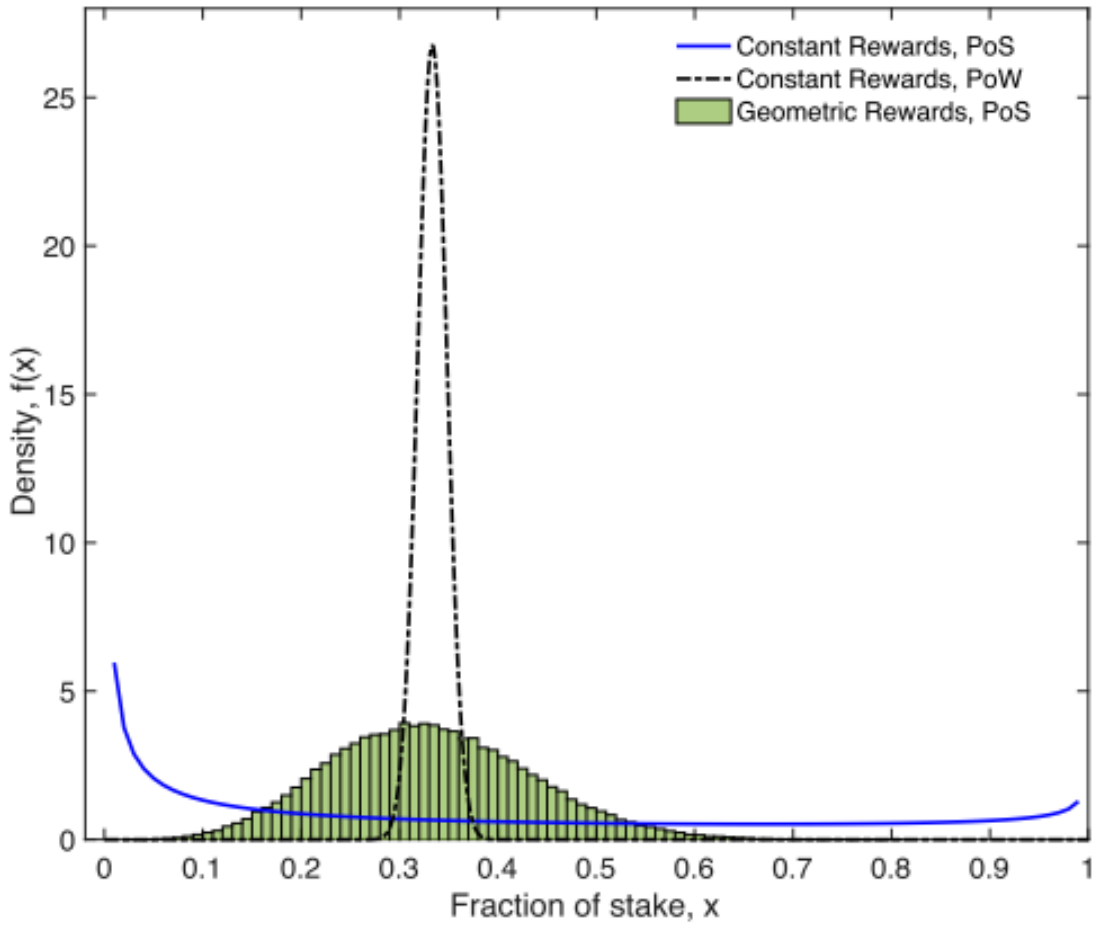
- Remark 1 – The maximum achievable variance is

$$\sup_{T \in \mathbb{Z}^+} \sup_{r} \mathrm{Var}(v_{A,r}(T)) \quad = \quad v_A(0)(1 - v_A(0))$$

- Remark 2 – If reward function r is $\boldsymbol{\varepsilon}$-equitable, r is also $\tilde{\boldsymbol{\varepsilon}}$-equitable

$$\tilde{\boldsymbol{\varepsilon}} \triangleq \mathbf{1} \cdot \min_{i \in [m]} \varepsilon_i$$

Geometric Block Reward



Geometric Block Reward Function

- Calculated from equitability
- Geometric Reward is the most equitable among functions that dispense R tokens over time T
- Dispense small rewards in the beginning when the stake pool is small
  - A single block reward cannot substantially change the stake distribution

Geometric Block Reward Function

$$\begin{aligned} \text{minimize}_{r\in\mathbb{R}^T} \quad & \mathrm{Var}(v_{A,r}(T)) \\ \text{s.t.} \quad & \sum_{n\in[T]} r(n) = R \\ & r(n) \geq 0\ ,\ \forall n \in [T]. \end{aligned}$$

->Affine Transformation and take log->

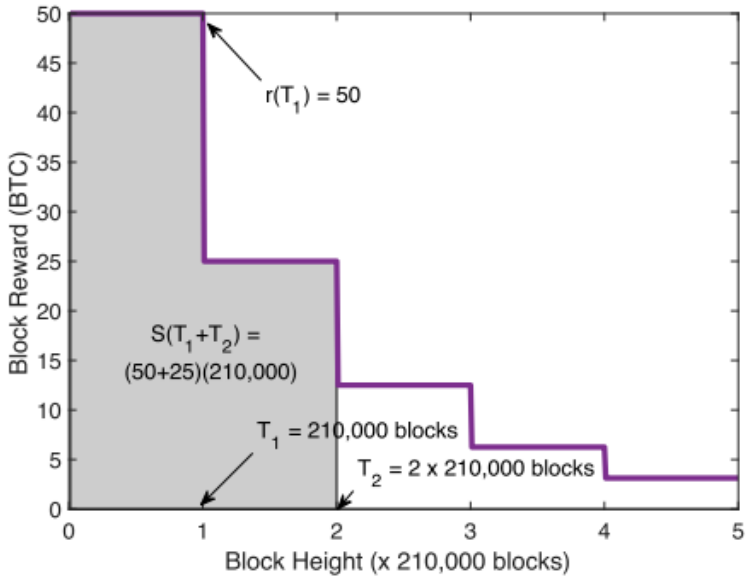
$$\begin{aligned} \text{maximize}_{\theta\in\mathbb{R}^T} \quad & \sum_{n=1}^{T} \log(2e^{\theta_n} - 1) \\ \text{s.t.} \quad & \sum_{n\in[T]} \theta_n = \log(1+R) \\ & \theta_n \geq 0, \forall n \in [T]. \end{aligned}$$

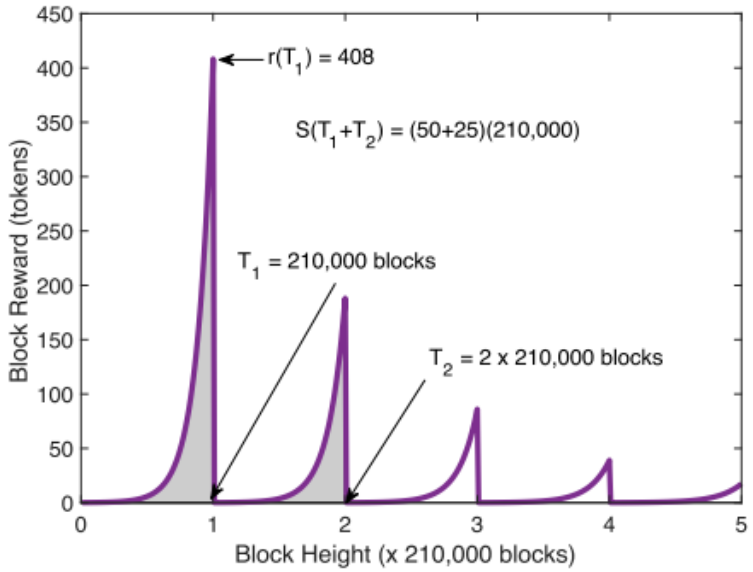
$$\begin{aligned} \frac{2e^{\theta_n}}{2e^{\theta_n}-1} - \lambda_n - \lambda = 0 \\ \lambda_n \geq 0 \\ \theta_n \lambda_n = 0 \end{aligned} \quad = \quad \theta^* = ((\log(1+R))/T)$$

Geometric Block Reward Function

- Block reward r(n) is ultimately an incentive
  - Should compensate nodes for the resources cost of proposing blocks

$$r_g(n) := (1+R)^{\frac{n}{T}} - (1+R)^{\frac{n-1}{T}}$$





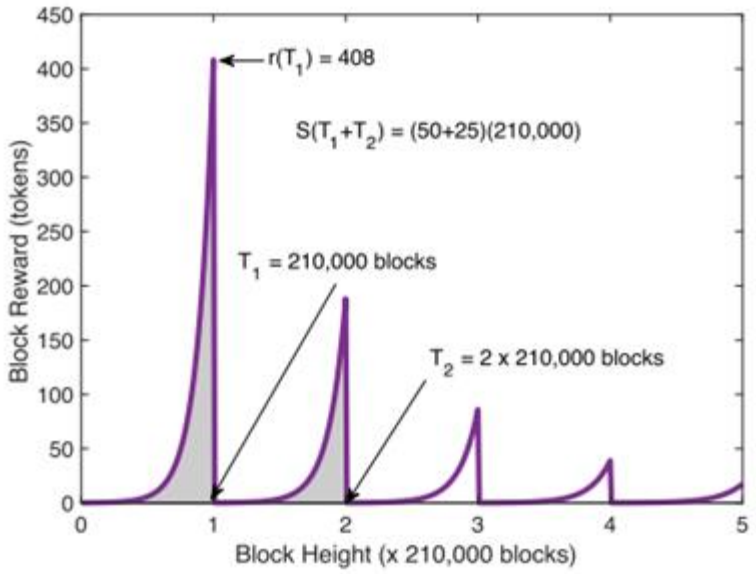
Equitability for a single time interval

- Over time T it is fair, but what about single time interval?
- Proposers may leave the system
- In this manner, geometric may not be optimal
- A sequence of checkpoints will yield a different most equitable function

$$r(n) = (1 + \tilde{R}_{i-1}) \left(\left(\frac{1 + \tilde{R}_i}{1 + \tilde{R}_{i-1}} \right)^{\frac{n - T_{i-1}}{T_i - T_{i-1}}} - \left(\frac{1 + \tilde{R}_i}{1 + \tilde{R}_{i-1}} \right)^{\frac{n-1 - T_{i-1}}{T_i - T_{i-1}}} \right)$$

Other problems

- Geometric reward function does not mitigate the effects of compounding when strategic actors are present
- Dramatic fall of incentives may repel miners



Analysis

Equitability of Stake Pools

- A single party A with $V_A(0)$ fraction of stake joins a pool P with $V_P(0)$

$$\mathrm{Var}(v_{A,r}(T)) = \left(v_A(0) - v_A(0)^2\right)\left(1 - \frac{S(0)^2}{S(T)^2}\prod_{n=1}^{T}(2e^{\theta_n} - 1)\right)$$

Equitability of Stake Pools

- A single party A with $V_A(0)$ fraction of stake joins a pool P with $V_P(0)$

$$\mathrm{Var}(v_{A,r}(T)) = \left(v_A(0) - v_A(0)^2\right)\left(1 - \frac{S(0)^2}{S(T)^2}\prod_{n=1}^{T}(2e^{\theta_n} - 1)\right)$$

Equitability of Stake Pools

- A single party A with $V_A(0)$ fraction of stake joins a pool P with $V_P(0)$

$$\begin{aligned}\mathrm{Var}(v_{\tilde{A},r}(T)) &= \left(\frac{v_A(0)}{v_P(0)}\right)^2 \left(v_P(0) - v_P(0)^2\right)\left(1 - \frac{S(0)^2}{S(T)^2}\prod_{n=1}^{T}(2e^{\theta_n} - 1)\right) \\ &= \frac{1 - v_P(0)}{v_P(0)}\,\frac{v_A(0)}{1 - v_A(0)}\mathrm{Var}(v_{A,r}(T))\ .\end{aligned}$$

- Party A's variance reduces by a factor of $(v_P(0)/v_A(0))((1 - v_A(0))/(1 - v_P(0)))$

Equitability of Stake Pools

- A single party A with $V_A(0)$ fraction of stake joins a pool P with $V_P(0)$

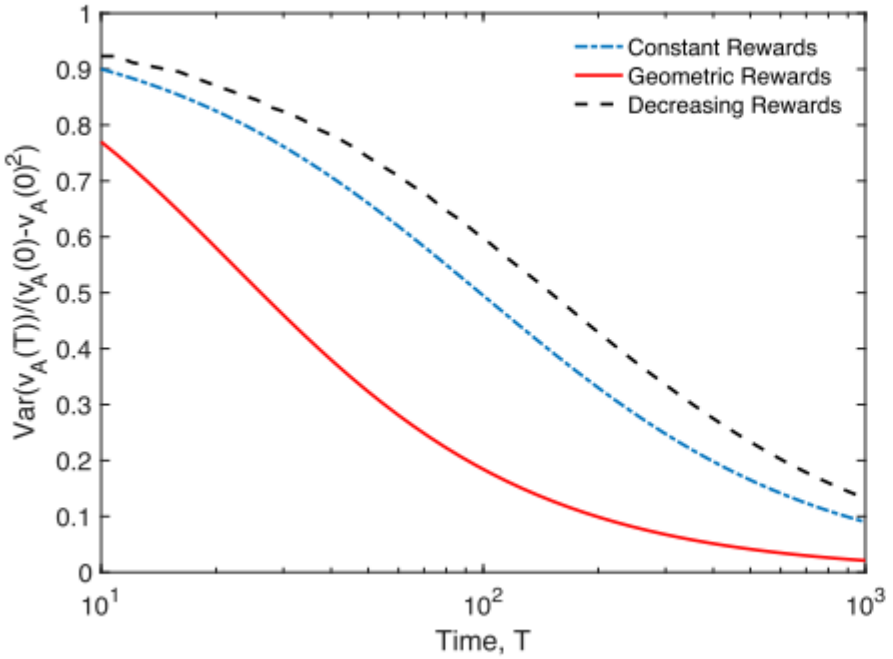
$$\mathrm{Var}(v_{\tilde{A},r}(T)) = \left(\frac{v_A(0)}{v_P(0)}\right)^2 \left(v_P(0) - v_P(0)^2\right)\left(1 - \frac{S(0)^2}{S(T)^2}\prod_{n=1}^{T}(2e^{\theta_n} - 1)\right)$$

$$= \frac{1 - v_P(0)}{v_P(0)}\frac{v_A(0)}{1 - v_A(0)}\mathrm{Var}(v_{A,r}(T)) \ .$$

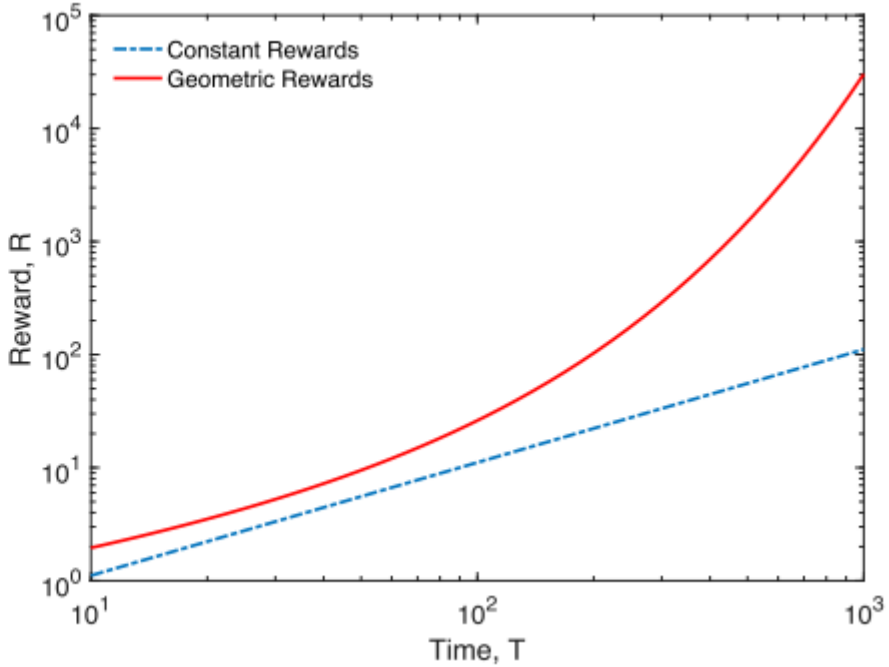
- Party A's variance reduces by a factor of $(v_P(0)/v_A(0))((1 - v_A(0))/(1 - v_P(0)))$
- == Equitability increases by a factor of
- Geometric function still holds its position as an optimal solution

Comparison between other functions

Smaller is better



Which is better?



- The results suggest that in a PoS system, a large initial stake pool can actually help to ensure equitability

Strategic Behavior

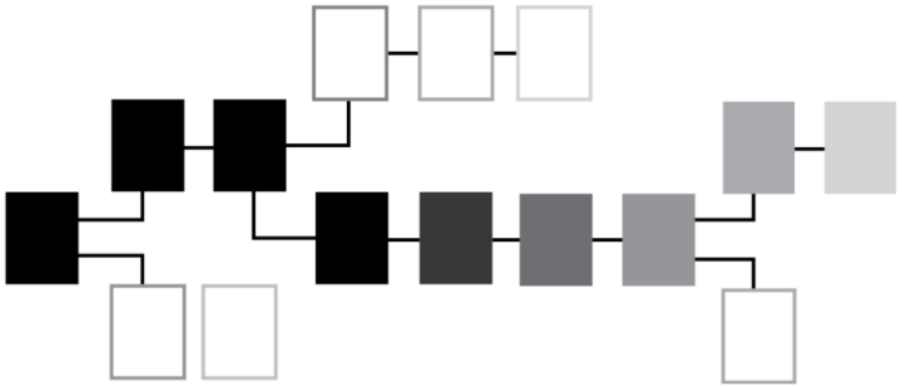
Strategic Behavior

- Adversary A wants to maximize its fraction of the total stake in the main chain

$$v_A(t) = \frac{|\{n \in [T] : (W(n) = A) \wedge (B_T(n) \neq \emptyset)\}|}{\ell_T}$$

- Maximize by choosing when and where to append its blocks.

- Forking does not cost

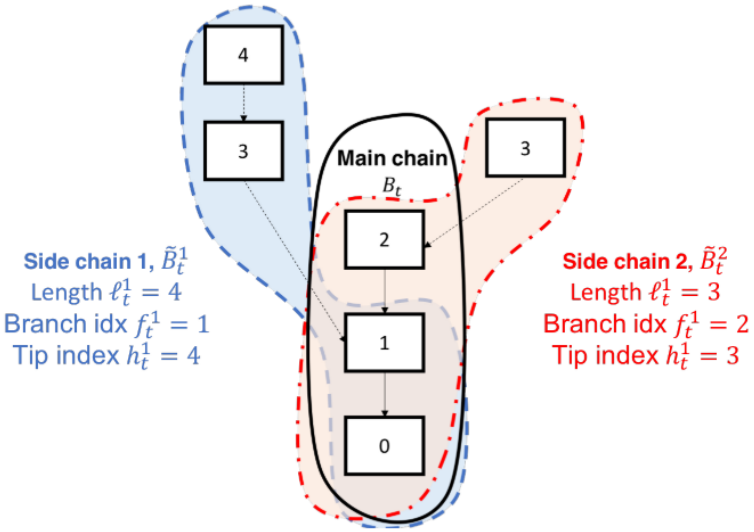


Strategic Behavior

- Adversary can build arbitrarily many side-chains branching from anywhere
- Block rewards are also withheld for those adversarial blocks held aside to build side-chains
- Under compounding, delaying the rewards of such side-chains costs the adversary in the following proposer elections, as the adversary is the much less likely to be elected as a leader
- Needs to balance the gain in keeping a log side-chain and the loss in intermediate leader elections

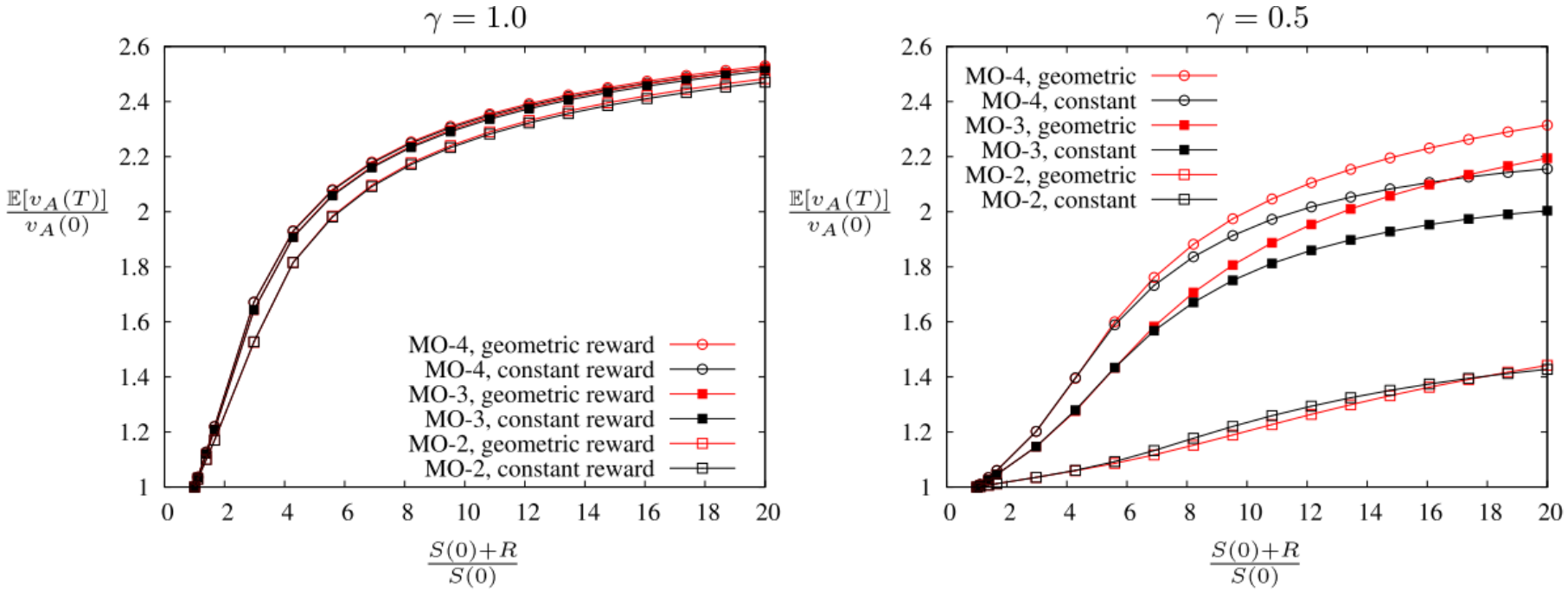
MO-k (Match-Override – k)

- When honest block is generated
  - It adversary has a side chains that is longer than the main chain, open the earliest branched chain to matching point and discard all the other side chains
  - No such chains, wait and all side chains are discarded
- When adversary block is generated
  - Append it to every side chains, start new side chain from top if none exists.
  - If a side chain exists from top of main chain and the blocks exceed k, release the chain



MO-k (Match-Override – k)

- Adversary's relative fractional stake approaches 3 as total reward R increases.
- Just like PoW when well connected, much effective



Strategic Behavior (Solution)

- For Ethereum a proposer "Slasher" allows punishment of miners who attempt to fork
  - Using stake to mine requires signing the current block with the private key corresponding to the transactions making up the miner's stake
  - If a miner uses the same stake to sign two inconsistent chains, other miners enter these two signatures later on in the bock chain as proof of misbehavior and collect a portion of this stake as a bounty
- Checkpointing
  - Nodes receive regular checkpoint updates from designated checkpoint nodes, signed by a designated private key
  - Nodes will discard branches that conflict with checkpoints
  - This allows operator to pick a winner in case of a fork and even 'roll back' blocks
  - Interesting design but no longer a decentralized consensus protocol

Conclusion

Summing Up

Equitability

== Variance

Smaller the better

Great metric to compare reward functions

Changing stakes? Reduce epoch, coin-age

Negative effect of compounding can be reduced by carefully choosing parameters

Geometric Function

The most equitable reward function

The total block rewards disseminated in each epoch should be small compared to the initial stake pool size

May not be desirable with drastic changes in between epoch

MO-k

Strategic behavior is especially effective in PoS

Probably not a matter of reward function

Designing incentive-compatible consensus protocol for strategic participants may be the right approach

Thank You