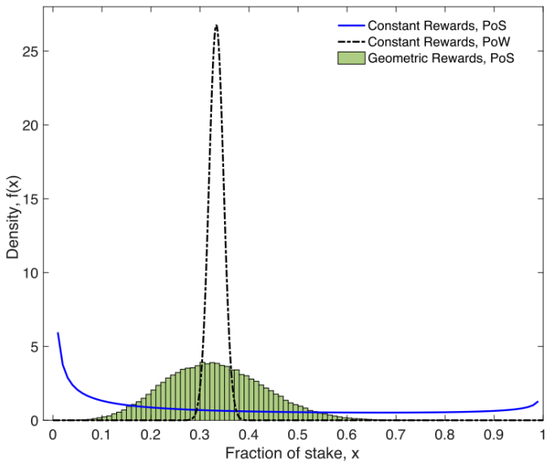
Random Rewards in Proof-of-Stake Protocols

Dominik Harz‡ and **Ryuya Nakamura***†

‡Department of Computing, Imperial College London, *Faculty of Engineering, The University of Tokyo, †R&D, LayerX

Motivation: Wealth Compounding subverts Blockchain Consensus Security



Proof-of-Stake requires validators to stake currency to participate in the consensus protocol. The consistency and liveness of PoS consensus protocols depends on the fact that at most 1/2 or 1/3 of validators are malicious.

However, **wealth compounding** occurs in PoS protocols such that fairness does not hold over an infinite time horizon [1]. Validators **naturally accumulate either no or all stake,** and hence the security assumptions of PoS protocols is subverted.

Equitability considers an infinite time horizon, but its optimal reward function, geometric rewards, introduces large **reward gaps** susceptible to the "gap game" [2] where validators can game the protocol.

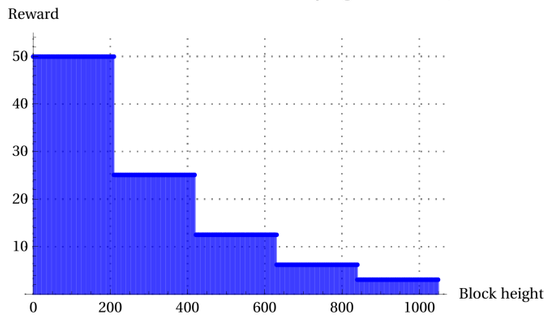
Figure 1: Wealth compounding for constant PoW, constant PoS, and geometric PoS reward functions [1].

Background: Fairness and Equitability

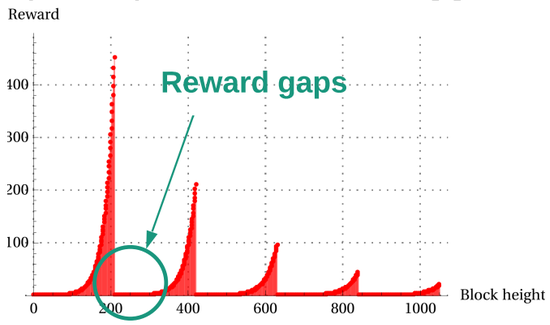
Fairness: A blockchain has δ-approximate fairness if with high probability honest parties controlling Φ of the stake receives (1-δ)/Φ shares of the reward [3]. However, this does not hold for PoS systems since rewards can be used as stake for the next round.

Equitability: The ε-equitability of a reward function depends on the variance of the reward over time. If for the same rewards, one of two reward functions shows lower variance it is more equitable given the same initial stake distribution [1].

Constant reward function (e.g. Bitcoin, Ethereum)

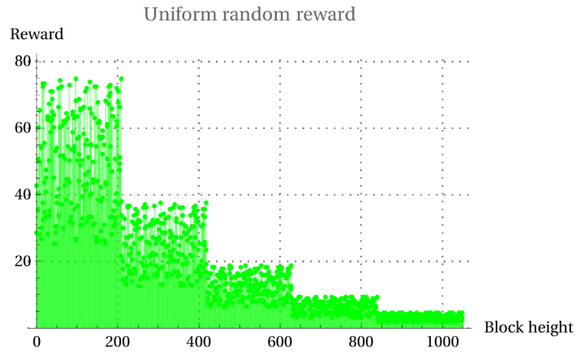


Optimal equitable reward function [1]

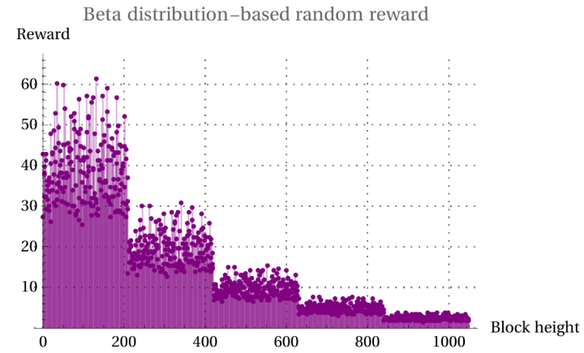


Contribution: Random reward functions

Hypothesis: Random reward functions prevent selfish minining due to uncertainty and can reduce variance compared to constant reward functions.

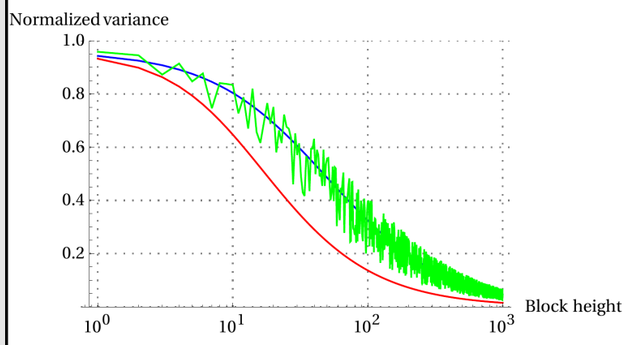


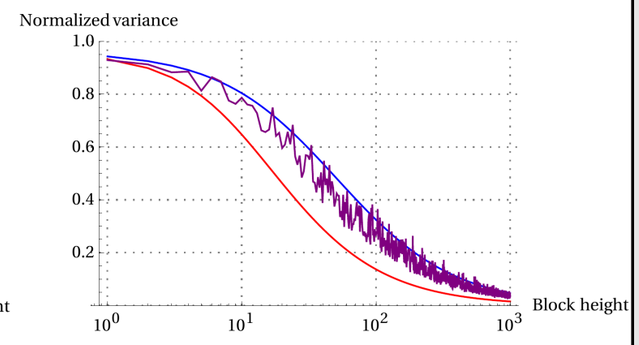
Uniform random reward function over [0.5, 1.5)



Random reward with beta distribution with α = 2 and β = 5 over [0.5, 1.5).

Contribution: Reducing variance without introducing large gaps





Preliminary result: Uniform random functions are similar to constant functions in terms of variance. Beta distributions are a likely candidate to reduce variance while keeping the gap between rewards small.

Conclusion

Equitability: Random reward functions based on beta distributions seem to reduce variance i.e. have higher equitability than constant reward functions.

Selfish mining: Although the equitability of beta distribution-based reward functions is worse than the optimal geometric reward function, it reduces the selfish mining opportunities. Proof left as future work.

[1] Fanti, G., Kogan, L., Oh, S., Ruan, K., Viswanath, P., & Wang, G. (2019). Compounding of Wealth in Proof-of-Stake Cryptocurrencies. In Financial Cryptography and Data Security 2019.
[2] Tsabary, I., & Eyal, I. (2018). The Gap Game. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security - CCS '18 (pp. 713–728). New York, New York, USA: ACM Press.
[3] Pass, R., & Shi, E. (2017). FruitChains: A Fair Blockchain. In Proceedings of the ACM Symposium on Principles of Distributed Computing - PODC '17 (pp. 315–324). New York, New York, USA: ACM Press.
[4] Eyal, I., & Sirer, E. G. (2014). Majority Is Not Enough: Bitcoin Mining Is Vulnerable. In Financial Cryptography and Data Security 2014 (Vol. 8437, pp. 436–454). Berlin, Heidelberg.