Poster: Random Rewards in Proof-of-Stake Protocols

Dominik Harz[1] and Ryuya Nakamura[2,3]

[1] Department of Computing, Imperial College London
d.harz@ic.ac.uk
[2] Faculty of Engineering, The University of Tokyo
[3] Research and Development, LayerX
ryuya.nakamura@layerx.co.jp

1 Introduction

Bitcoin introduced the idea of providing monetary rewards for participating in its Proof-of-Work (PoW) Sybil-resistance mechanism [4]. The reward a miner receives is intended to be *proportional* to the work a miner provides in the system. However, selfish mining strategies allow miners to almost double their fair share of rewards [2]. As a response, new reward schemes are proposed that distribute rewards *approximately fair* such as Fruitchains [5]. Fruitchains creates a δ-approximate Nash equiblibrium in which miners controlling a fraction of the mining power will get a guaranteed fraction over a specified period. Although initially designed for PoW, Fruitchains has been adopted for Proof-of-Stake (PoS) systems as, for example, in Snow White [1].

PoS constructions, however, follow a Pólya urn process. A validator can use its reward immediately to increase its share for the next voting round, thus compounding its wealth [3]. This ultimately reduces the security of the blockchain: PoS protocols require a minimum set of honest validators to provide consistency and liveness. With wealth compounding, validator monopolies are naturally created whereby a small set or even a single validator gains enough stake to arbitrarily control the ledger. As a remedy, Fanti et al. introduce a geometric reward function and prove that it is optimal with regards to *equitability* [3]. The ϵ-equitability of a reward function depends on the variance of the reward over time, where lower variance is desirable. However, their optimal geometric reward function introduces large inequalities in rewards between any two epochs, leading to instability of the chain due to selfish mining strategies.

We introduce and evaluate two random reward distribution functions that should be equitable and, at the same, provide a smaller inequality of reward between epochs.

2 Random reward functions

The core idea of our proposal is to randomize rewards. Validators in PoS systems are chosen at random, as such, they never know when the get to propose a block and reap a reward. However, we can also randomize the *amount of the reward*. Intuitively, this allows us to reduce the drastic change between epochs while introducing a measure to reduce wealth compounding: even if a validator is more likely to be chosen as a block proposer, we can reduce the likelihood of having a large reward. Formally, we adopt

the constant reward function r_c as comparable in Bitcoin and apply a randomization parameter x. The parameter R is the total reward in an epoch and T gives the length of an epoch in number of blocks:

$$r_c = \frac{xR}{T} \tag{1}$$

Uniform random rewards We apply a uniform random distribution $[0.5, 1.5)$ to the parameter x. We choose such that, on average, the total reward amount is the same as with the constant reward function. Next, we apply the equitability measurement of [3]. The reward difference between two epochs is random and unknown a priori, and hence, validators are less susceptible to selfish mining strategies. However, we observe that the normalized variance of the uniform distribution is, on average, equivalent to the constant reward function.

Beta distribution-based random rewards To improve the variance of the reward function, we apply a beta distribution with $\alpha > 1$ and $\beta > 1$ between $[0.5, 1.5)$. The intuition is to have the majority of rewards randomly drawn below 1, but to have the possibility to have relatively high rewards occasionally. Applying the equitability measurement of [3], we notice that the variance is improved compared the the constant reward function.

3 Conclusion

While Fanti et al. show that their geometric reward function is optimal, it is susceptible to selfish-mining and strategic behaviour [3]. We introduce a beta distribution-based random reward function that shows promise to balance equitability and resistance against selfish mining strategies. We leave formal proofs as future work.

References

1. Bentov, I., Pass, R., Shi, E.: Snow white: Provably secure proofs of stake. https://eprint.iacr.org/2016/919.pdf (2016), https://eprint.iacr.org/2016/919.pdf, accessed: 2016-11-08
2. Eyal, I., Sirer, E.G.: Majority Is Not Enough: Bitcoin Mining Is Vulnerable. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 8437, pp. 436–454. Berlin, Heidelberg (2014). https://doi.org/10.1007/978-3-662-45472-5_28, http://link.springer.com/10.1007/978-3-662-45472-5http://link.springer.com/10.1007/978-3-662-45472-5_28
3. Fanti, G., Kogan, L., Oh, S., Ruan, K., Viswanath, P., Wang, G.: Compounding of Wealth in Proof-of-Stake Cryptocurrencies. In: Financial Cryptography and Data Security (2019), http://arxiv.org/abs/1809.07468
4. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008)
5. Pass, R., Shi, E.: FruitChains: A Fair Blockchain. In: Proceedings of the ACM Symposium on Principles of Distributed Computing - PODC '17. pp. 315–324. ACM Press, New York, New York, USA (2017). https://doi.org/10.1145/3087801.3087809, http://dl.acm.org/citation.cfm?doid=3087801.3087809