Problem set 7: Proof of Stake

1 Proof of stake

In this problem set, we will examine the financial differences between different mechanisms to choose which miner adds the next block. We will prove and expand on results from lecture.

a) Consider a proof of work system with n miners, each of which has hash power h_i. Assume that the hash power is fixed and random (*i.e.*, there is no 'reinvestment' of rewards and the probability of earning the next block is uniform over the available hash power). Fix the per-block reward to be 1 token. Show that the distribution of miner i's fraction of earnings after T blocks is $\text{Binom}(T, h_i/\sum_j h_j)$. Plot this for some values of h_i and T.

Proof of stake is a popular alternative to proof of work. We consider a setup where each miner starts with stake $\pi_i(0)$ For convenience, assume that $\sum_i \pi_i(0) = 1$. At each time step $t = 1, \ldots, T$, some block reward $r(t)$ is given to the miner that 'wins' the block. The miner i is chosen proportional to their stake, *i.e.*, the probability that miner i is chosen is π_i, and this reward is continuously reinvested (*i.e.*, if i mines, the block, then $\pi_i(t+1) \leftarrow \pi_i(t) + r(t)$). We assume that $\sum_{t=1}^{T} r(t) = T$.

b) Show that, under any block reward $r(t)$, $\mathbf{E}\left[\pi_i(T)\right] = \pi_i(0)$. (Aside: This type of process is called a *martingale* and has a number of useful properties.)

c) Fix $r(t) = r$ for all t. What is the probability that miner i will win exactly k of the next n blocks?

Without much additional work[1], we can prove that the fraction of miner i's reward as $n \to \infty$ is beta distributed (`https://en.wikipedia.org/wiki/Beta_distribution`) with parameters π_i, $1 - \pi_i$: $\text{Beta}(\pi_i, 1 - \pi_i)$.

d) Plot this distribution for some values of π_i. Comment on the distribution of wealth as $n \to \infty$. Why does this not conflict with your answer to part (b)? Is this behavior desirable?

Since we care about the distribution of staked wealth, we can define a measure of wealth inequality, for example

$$\text{ineq} = \frac{\text{Var}(\pi_i(T))}{\text{Var}(\pi_i(0))} = \frac{\text{Var}(\pi_i(T))}{\pi_i(0)(1 - \pi_i(0))}.$$

It's reasonable to find an update rule that minimizes ineq at time T, which we can write as the following optimization problem:

$$\begin{aligned} \text{minimize} \quad & \text{Var}(\pi_i(T)) \\ \text{subject to} \quad & \sum_{t=1}^{T} r(t) = T \\ & r(t) \geq 0, \end{aligned} \tag{1}$$

[1] Check out the Polya Urn model `https://en.wikipedia.org/wiki/Pólya_urn_model`

where the variables are the reward $r(t)$ and the distribution parameters $\pi_i(t)$, $t = 1, \ldots, T$. It turns out that the geometric update rule

$$r(t) = T(1+T)^{\frac{t-1}{T}},$$

is the variance minimizing update rule. This fact that be proved from the KKT conditions of (1). See [Fan+19] for details.

References

[Fan+19] Giulia Fanti et al. "Compounding of wealth in proof-of-stake cryptocurrencies." In: *International conference on financial cryptography and data security*. Springer. 2019, pp. 42–61.