# Proof of Less Work

BY CHENG WANG

## 1 Introduction

This paper is about PoLW to reduce the energy consumption of Nakamoto PoW[1]. This paper is inspired by the recent paper from Itay, Alexander and Ittay [2] which describes several algorithms with reduced external costs. It's also inspired by the white paper of Alephium project[3] which introduces dynamic mining rewards with lockup. We propose two algorithm (linear PoLW and exponential PoLW) which could reduce the energy consumption of Nakamoto PoW.

## 2 Linear PoLW

Let $W$ be the amount of work needed for one block. Let the maximal block reward be 1 coin. The miner could choose to get only $\alpha$ coin reward ($0<\alpha\leqslant 1$). If the actual work of the new block is $W'$, then the weighted work is $\left(1+\frac{1-\alpha}{\gamma}\right)W'$, where $\gamma\leqslant 1$ is a system parameter. Each miner could choose a different $\alpha$ to ample it's mining work. The idea is that the $1-\alpha$ coins are burned for some amount of weighted work.

| | |
|---|---|
| $W$ | amount of work needed for a regularly mined block |
| $W'$ | actual work the miner produces |
| $\alpha\leqslant 1$ | actual block rewards. maximal is 1 coin |
| $\beta$ | cost for regular block mining |
| $\gamma\leqslant 1$ | system parameter for weight calculation |

**Table 1.**

## 3 Mining Strategy

The question arises that which $\alpha$ should a miner use to maximize its return. Let's say a miner $M$ has $x$ coin to use for mining the block. Let $\beta$ coin be the resource cost of $W$ work for the regular Nakamoto mining. Then in the equilibrium case, the probability of $M$ getting the block is

$$p_M=\frac{x\{1+(1-\alpha_M)/\gamma\}}{\beta}$$

The expected return is

$$p_M\alpha_M-x=\left(1+\frac{1-\alpha_M}{\gamma}\right)\alpha_M\frac{x}{\beta}-x$$

The maxmized return is

$$\max\left(p_M\alpha_M-x\right)=\max\left(\left(1+\frac{1-\alpha_M}{\gamma}\right)\alpha_M\right)\frac{x}{\beta}-x$$

We could easily deduce that

$$\alpha_M=\frac{1+\gamma}{2}$$

Therefore, the long term strategy $\mathcal{S}$ for a miner is to set $\alpha$ to be $\frac{1+\gamma}{2}$ to mine new blocks. However, in short term, the miner could adjust its $\alpha$ for better expected return. We show that strategy $\mathcal{S}$ is an equilibrium strategy by an ideal analysis.

Note that even if the Miner $M$'s mining algorithm or machine is more efficient than the others, the optimal value of $\alpha_M$ is still $\frac{1+\gamma}{2}$.

## 4 Equilibrium Strategy

Let's assume that all the miners work together and use the same $\alpha$ to try to maximize the return of mining. In order to make the weighted work reach the target work $W$, the miners need to cost $\frac{\beta}{1+(1-\alpha)/\gamma}$ coin. The actual return of the miners is

$$R(\alpha) = \alpha - \frac{\beta}{1+(1-\alpha)/\gamma}$$

With some calculation, we get the following result

$$\max R(\alpha) = \left| \begin{array}{cl} 1+\gamma-2\sqrt{\beta\gamma} & \text{when } \gamma \leqslant \beta \leqslant \dfrac{(1+\gamma)^2}{4\gamma}, \text{with } \alpha = 1+\gamma-\sqrt{\beta\gamma} \\ 1-\beta & \text{when } \beta < \gamma, \text{with } \alpha = 1 \\ 0 & \text{when } \beta > \dfrac{(1+\gamma)^2}{4\gamma}, \text{donot mine} \end{array} \right.$$

We see here that when the mining cost is very low, the miners will set $\alpha = 1$ and it degenerates to the classic Nakamoto mining. However, as the mining cost goes up, the miners will have to set $\alpha = 1+\gamma-\sqrt{\beta\gamma}$ to maxize its return. Therefore, we see that in the non-equilibrium case, the miners could set $\alpha$ to be different from $\frac{1+\gamma}{2}$ for better mining return.

**Equilibrium Case.** In equilibrium, $\max R(\alpha)$ should be equal to 0. In such case, we have $\beta > \gamma$ and $1+\gamma-2\sqrt{\beta\gamma} = 0$. Therefore

$$\begin{aligned} \beta &= \frac{(1+\gamma)^2}{4\gamma} \\ \alpha &= 1+\gamma-\sqrt{\beta\gamma} = \frac{1+\gamma}{2} \end{aligned}$$

We now show that $\alpha$ will be $\frac{1+\gamma}{2}$ for all the miners in the equilibrium case. Therefore, $\mathcal{S}$ is the equiliblrium strategy in the case where mining is negligible to 0.

## 5 Security Analysis

We only compare our algorithm to the classic Nakamoto PoW algorithm to see the security differencies. In Nakamoto PoW, an attacker needs to first invest 1 coin to mine a new block and then get the reward back in the equilibrium case.

In our new algorithm, the cost for an attacker $A$ to mine a new block with $\alpha_A$ is

$$\mathrm{Cost}_A = 1 - R_A = 1 - \alpha_A + \frac{\beta}{1+(1-\alpha_A)/\gamma}$$

In equilibrium where $\beta = \frac{(1+\gamma)^2}{4\gamma}, \alpha = \frac{1+\gamma}{2}$, the cost of the attacker is $2\sqrt{\beta\gamma} - \gamma = 1$. Therefore, we show that our new PoWW algorithm has same security as Nakamoto PoW in terms of new block generation cost.

We ignore the other metrics analysis similar to that of paper [2], which should be intuitive.

## 6 Energy consumption.

The actual work done by the miner is $\frac{\beta}{1+(1-\alpha)/\gamma}$ coin. In equilibrium where $\beta = \frac{(1+\gamma)^2}{4\gamma}, \alpha = \frac{1+\gamma}{2}$, the work amount is equal to the mining reward $\frac{1+\gamma}{2}$, less than 1 coin. Therefore, it costs less energy compared to Nakamoto PoW.

## 7 Generalization & exponential PoLW

Let's assume now that the weights of work is calculated by $1+f(1-\alpha)$. In our previous analysis, $f=\frac{1-\alpha}{\gamma}$. Similarly, let's first find out the optimal $\alpha$ for miners in long term.

$$p_M = \frac{x\{1+f(1-\alpha_M)\}}{\beta}$$

The expected return is

$$p_M\alpha_M - x = \{1+f(1-\alpha_M)\}\alpha_M\frac{x}{\beta} - x$$

The maxmized return is

$$\max(p_M\alpha_M - x) = \max(\{1+f(1-\alpha_M)\}\alpha_M)\frac{x}{\beta} - x$$

The optimal mining parameter would be better to satisfy the following equation of derivative.

$$1 - f'(1-\alpha_M)\alpha_M + f(1-\alpha_M) \;=\; 0$$

We want to choose good function $f$ such that $0<\alpha_M<1$. As in the equilibrium case, the energy cost would be close to $\alpha_M$, we also want the optimal $\alpha_M$ to be small if possible. There might be many ways to choose such kind of functions. We focus on this following simple case.

**Case $f(1-\alpha) = e^{\gamma(1-\alpha)} - 1\ (\gamma \geqslant 1)$.** In this case, we have

$$\max(\{1+f(1-\alpha_M)\}\alpha_M) \;=\; \max(\alpha_M e^{\gamma(1-\alpha_M)})$$

With simple calculation, we know that the optimal $\alpha_M = \frac{1}{\gamma}$.

In the following, we apply the similar analysis as before, without repeating all the details.

**Equilibrium.** The actual return of miners is

$$R(\alpha) = \alpha - \beta e^{-\gamma(1-\alpha)}$$

$$R'(\alpha) \;=\; 1 - \beta\gamma e^{-\gamma(1-\alpha)}$$

$$\max R(\alpha) = \begin{cases} \alpha - \frac{1}{\gamma} & \text{when } \beta \geqslant \frac{1}{\gamma}, \text{with } \alpha = 1 - \frac{\lg(\beta\gamma)}{\gamma} \\ 1-\beta & \text{when } \beta < \frac{1}{\gamma}, \text{with } \alpha = 1 \end{cases}$$

In equilibrium, we have $\alpha - \frac{1}{\gamma} = 0$ and $\alpha = 1 - \frac{\lg(\beta\gamma)}{\gamma}$, therefore

$$\beta \;=\; \frac{e^{\gamma+1}}{\gamma}$$
$$\alpha \;=\; \frac{1}{\gamma}$$

Therefore, using $\alpha = \frac{1}{\gamma}$ is an equilibrium mining strategy.

**Security.** The cost of Attack $A$ is

$$\mathrm{Cost}_A = 1 - R_A = 1 - \alpha_A + \beta e^{-\gamma(1-\alpha_A)}$$

In equilibrium, the cost is 1 coin.

**Energy consumption.** In equilibrium, the actual mining cost (i.e. energy consumption) is $\frac{1}{\gamma}$. If we choose $\gamma$ to be large enough, this could be close to 0.

### 8 Parameter Selection

Let's call our two PoLW algorithms as linear PoLW ($f = \frac{1-\alpha}{\gamma}$, $\gamma \leqslant 1$) and exponential PoLW ($f(1-\alpha) = e^{\gamma(1-\alpha)} - 1, \gamma \geqslant 1$).

In linear PoLW, we could choose $\gamma$ close to zero so that the energy cost could be reduce to close to $\frac{1}{2}$. However, when $\gamma$ is small, the weight $1 + \frac{(1-\alpha)}{\gamma}$ to the actual mining work would be huge, this will make double spending more feasible with less actual mining work.

Same in exponential PoLW, we could choose $\gamma$ large so that the energy cost could be reduced to close to 0. However, when $\gamma$ is big, the weight $e^{\gamma(1-\alpha)}$ to the actual minging work would be huge, this will make double spending more feasible as well.

One way to ease this issue is to set the lower bound of $\alpha$ to be the optimal $\alpha$. When mining is in equilibrium, the attackers could not get better weight than the other miners.

The issue is still serious before mining reaching a equilibrium state. One possible solution is to adjust $\gamma$ when the blockchain evolves, so that the weights are lower from the beginning, but getting higher eventually. For example, we could adjust $\gamma$ based on the currently work target.

### 9 Implementation considerations.

The only thing to change is to use weighted work instead of the classic work. Therefore, there is neglagible implementation overhead.

### 10 Discussion.

It would be good to analysis PoLW in more complicated models.

## Bibliography

**[1]** Satoshi Nakamoto et al. Bitcoin: a peer-to-peer electronic cash system. 2008.

**[2]** Itay Tsabary, Alexander Spiegelman, and Ittay Eyal. Just enough security: reducing proof-of-work ecological footprint. *ArXiv preprint arXiv:1911.04124*, 2019.

**[3]** Cheng Wang. Alephium: a scalable cryptocurrency system based on blockow. https://github.com/alephium/white-paper/raw/master/white-paper.pdf, 2018.