Hello Everyone,

I propose an improved mining algorithm called PoLW to reduce the energy consumption of Nakamoto mining. One of the PoLW algorithms in the paper could reduce energy consumption by an arbitrary factor in equilibrium. (It's inspired by the recent and great work from Itay, Alexander, and Ittay [https://arxiv.org/abs/1911.04124] and one of my previous work.)

The key idea is to shift part of the external costs of mining to internal costs inside the network. In PoLW, the miners are able to give up part of the coin rewards so as to get weight (> 1) for the mining work they have done. Let's give more details below. For better description and analysis, please check out my little paper here [https://github.com/alephium/research/raw/master/polw.pdf].

Let's say in a PoW system, the normal block reward is 1 coin and the work required is W. In Nakamoto mining, the miners mine a block with work > W and take the block reward. In PoLW, a miner could choose to get less reward, let's say \alpha

(0 < \alpha <= 1

). By giving up a portion of the reward, the miner gets a weight 1+ f(1 - \alpha

). If the work of a new block the miner generates is W'

, then the weighted work of the block is (1 + f(1 - \alpha))W'

. If this weighted block reaches the block mining target, the miner could claim \alpha coin as reward.

In my paper, I discussed two PoLW algorithms: linear PoLW with f(1- \alpha) = (1 - \alpha)/\gamma

; and exponential PoLW with f(1 - \alpha) = e^{\gamma(1 - \alpha)} - 1

. In equilibrium of linear PoLW, miners would choose \alpha

as (1 + \alpha) / 2

to maximize the return, so the energy consumption could be reduced by a factor close to 1/2. While in equilibrium of exponential PoLW, miners would choose \alpha

as 1/\gamma

to maximize the return, so in theory the energy consumption could be reduced by a factor close to 0.

In practice, it takes a very long time to reach the equilibrium state and hash rate is dynamic always. The system could, however, update the system parameters (e.g. \gamma

) according to the actual mining work done by the miners.

Note: the conclusion is not that we could reduce the energy cost of Bitcoin/Ethereum to zero. That's gonna make the system attackable with existing mining powers level. The algorithms are gonna help the existing/new system based on PoW to reduce energy consumption gradually, especially for the future.

Looking forward to feedback and discussions.