A Novel Mechanism for Rewards Distribution in Pool Mining of Proof of Work

Keyang, Liu and Yukio, Ohsawa

the University of Tokyo, Graduate school of Engineering, Department of System Innovation

ABSTRACT

Proof of Work(PoW) as a critical consensus algorithm plays an essential role in Cryptocurrency fields. In normal PoW, computation power is the most vital resources. The security of a PoW system heavily relies on the computation power all honest users controlled. PoW systems distribute rewards among participants according to their contributions to the system as an incentive which is well known as digital currency. Users who pursues such rewards are known as miners. Miners can join pools to share and reduce the variance of their rewards. In this work, we will compare different reward distribution mechanisms in a long-term condition. The result shows that all existed mechanisms cannot motivate miners continuously mining in the pool. For solving this problem, a novel mechanism based on auction is proposed to improve the utility and motivation of miners. To our Best knowledge, this work is the first work focus on this problem and introduce auction into this field.

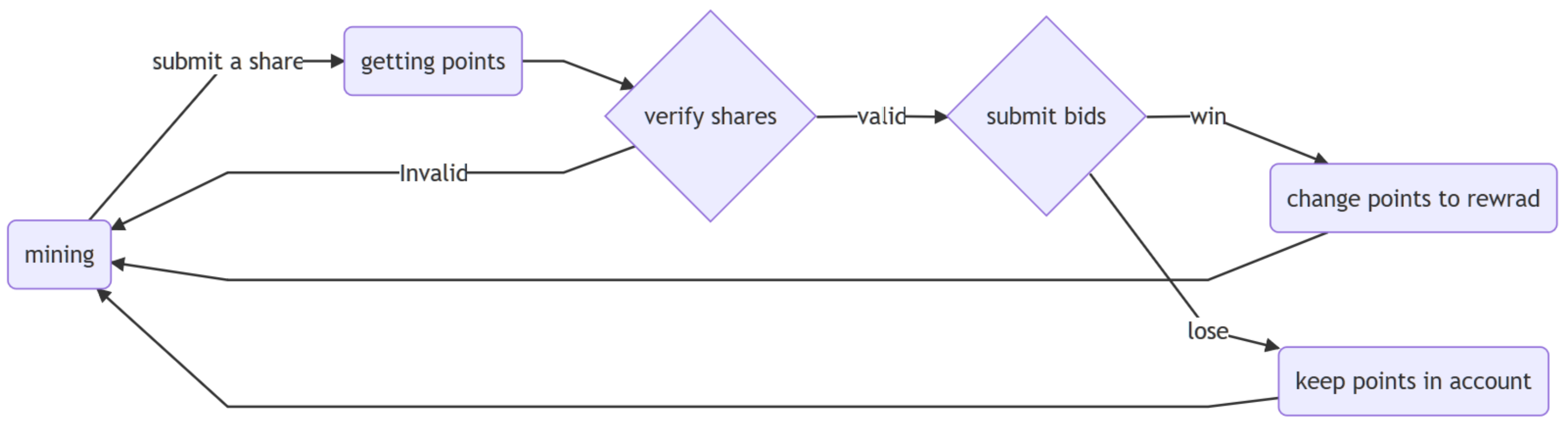
BACKGROUND

PoW is a consensus algorithm for maintaining the consistency of Blockchain systems. PoW gives up the using of communications, which is the core of traditional Byzantine Fault Tolerance (BFT) consensus algorithms. As a compensation, PoW uses a problematic competition to build a lottery for selecting the consensus to create a valid block. Although there are many different revised versions of PoW even using resources other than computation power, the logic behinds are still randomly select a participant to determine the block. If the possibility of solving the problem is too low, miners may not be able to tolerate the variance of return per try. Hence, miners can cooperate in organizing a pool for sharing risk and rewards. By doing this, the manager of a pool called pool operator. The pool operator should provide proper reward to miners in his pool.

Meni Rosenfeld proposed a model for analyzing reward system like Pay Per Share(PPS) and Pay Per Last N Shares(PPLNS). However, Meni's model cannot explain the real market well. First, the value of rewards significantly influenced the strategy of miners but not mentioned in his analysis. Second, the previous model treats reward in each round as a fixed number. Finally, the cost of mining is an important part of miner’s decision making. Under these conditions, miners can have a larger decision space and using hopping strategy to make higher profit.

In this work, miners can have different cost for mining and different evaluation to the reward. The reward mined out each time varied according to a distribution. Fundamentally, miners maximize their utility(reward * evaluation - cost) during mining. Besides, they will consider the risk they may take from the pool and the waiting time they suffered.

PROPOSAL



Our mechanism splits pool mining into two steps: 1. Whenever a miner submits a share, which represents some works have been done by the miner, pool operator will distribute a point to the miner. 2. When a miner's share create a valid block, the (parts) reward goes to the reward pool and an auction among all members will distribute it.

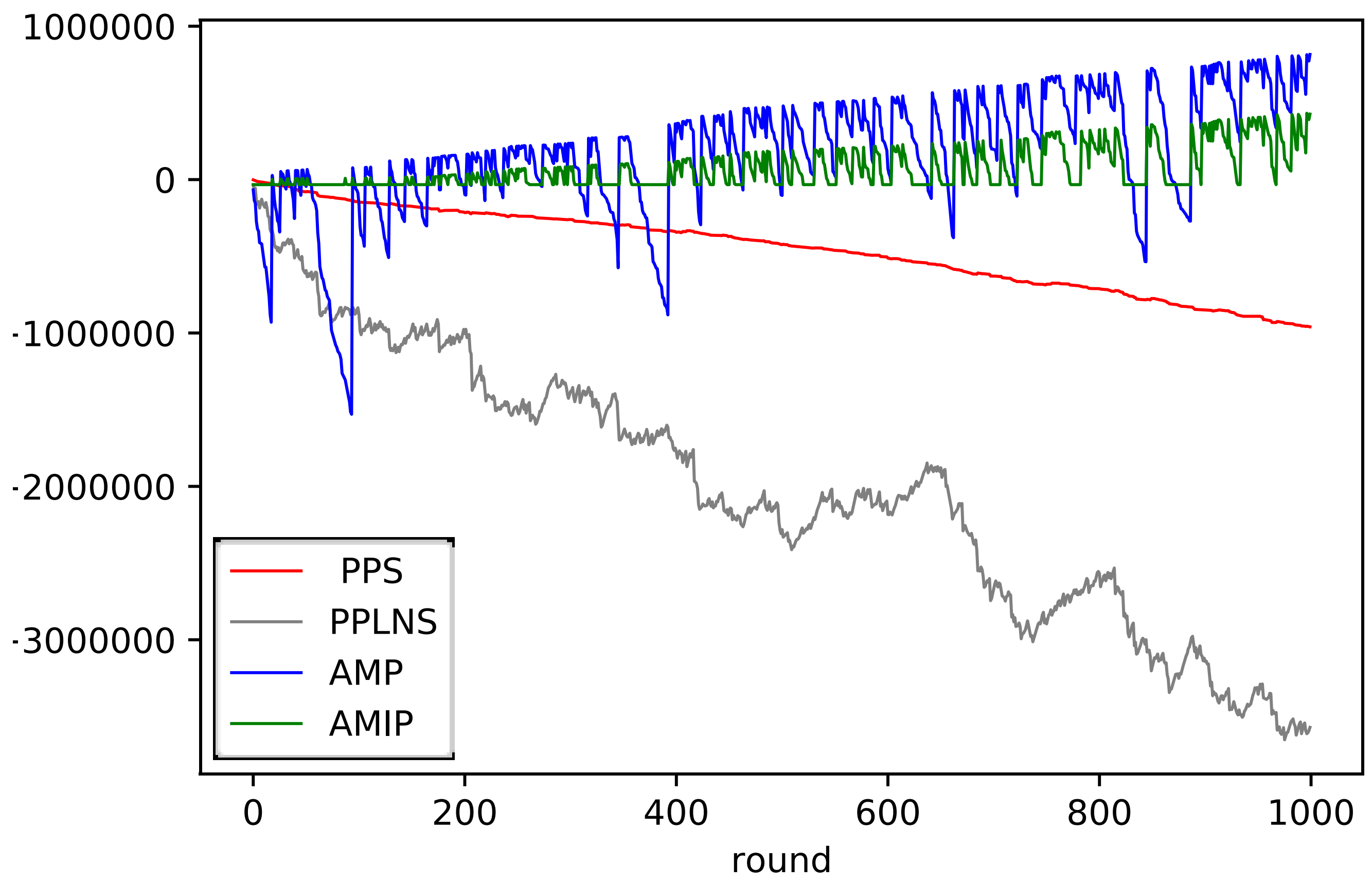
In an auction, rewards in the provided are divided into pieces. Each piece contains a unit rewards equals to the expected reward per share at the time. Each miner submits their bids and pool operator (or a distributed auction scheme) will run an auction to exchange miners’ points into pieces if they win the auction . Rest pieces not distributed will be moved back to the reward pool, and rest points remain in miner’s account. Miners are only allowed to submit one bid price, and there is a reserve price 1 (at least one share for one piece) as the lower bound. One old point(distributed in previous auctions) worth 1-f new points(distributed in this auction) during exchange.

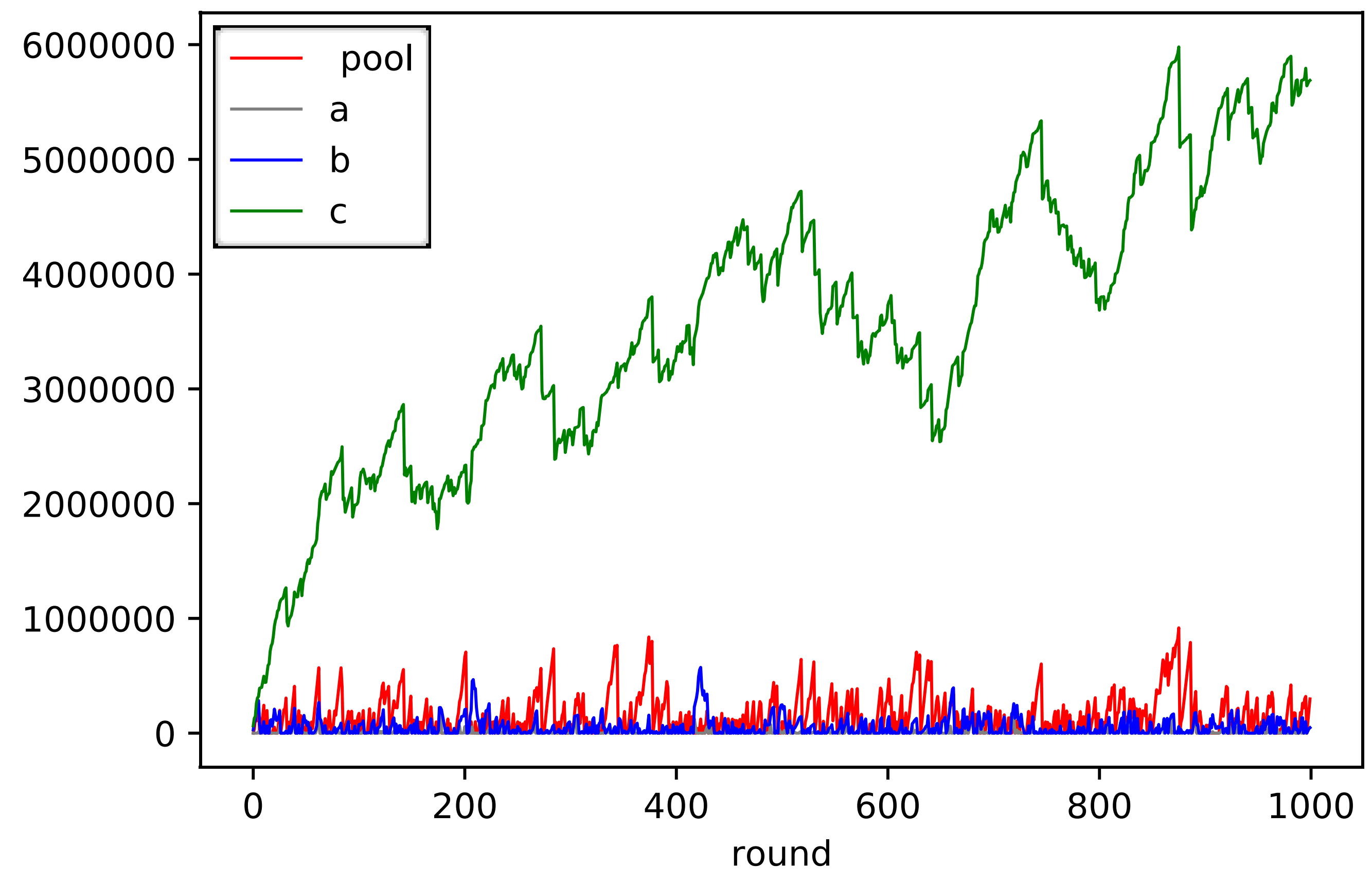
In auction model, the reward collected by pool is $B(t)$, and difficulty is $D(t)$. Hence, one piece contains $Z(t)=\frac{B(t)}{D(t)}$ rewards. Assume the miner’s minimum biding price is mp_i, his utility in the certain round will be:

$$U(T)=\int_0^T mp_i v(t)-m\big(v(t)\big)dt \le \int_0^T Z(t)v(t)-m\big(v(t)\big)dt$$

Where v(t) is the computation power at time t and m() is the cost of computation power. To maximize the utility, mp_i should equal to the marginal cost of increasing computation power. The upper bound of utility in this round is determined by $Z(t)$. However, a miner can decide not wining this time auction and preserve his point into next time, If $Z(t)<(1-f)E(Z(t))$. This strategy allows miner wait for future compensation. Since minimum price is determined by cost of mining, if a miner knows $E(Z(t))$ and $m()$, he can find out the utility he expects to get from the system and determines whether to mine in the system. The pool can get rid of hopping strategy if f is set carefully.

EXPERIMENT





To examine the result of our theory, we designed some simulation experiments to compare the utility of miners in different pool reward systems. As a conclusion, miners can earn much in PPLNS with a significant variance related to the luckiness. PPS can provide the most stable surplus for miners. Auction framework can provide more surplus to miners and follow the rule of more risks more surplus. If a miner stop mining at any time, he will get less compare to the miner who continue mining. However, miners may not be able to get a piece at reserve price all the time. In unlucky rounds, accumulating reserve points of high mp player(c) will force him to quit from the pool.

CONCLUSION

In this work, we propose the auction framework. In a pool use auction mechanism, miners can predict their surplus according to their minimum price and system condition. Indeed, this mechanism can be used not only in PoW but also other consensus algorithms. By designing a quantity variable for the cost of maintaining consensus, our work can provide a fair environment for participants, and make the system more robustness to attackers and more difficult for attacking. This work also provides many interest topics for considering: the dominant strategy of miners, the best auction rule, and the case of an unstable minimum price. Under these new scenarios, we may introduce more restrictions to the system.

REFERENCE

[1]Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

[2]Rosenfeld, M. (2011). Analysis of bitcoin pooled mining reward systems. arXiv preprint arXiv:1112.4980.

[3]Comparison of mining pools. Retrieved December 9, 2018, From: https://en.bitcoin.it/w/index.php?title=Comparison_of_mining_pools\&oldid=65140

[4]Hash Rate of Bitcoin System. Retrieved December 8, 2018, From: https://bitinfocharts.com/comparison/bitcoin-hashrate.html

[5]Patrick O'Brien, Are transaction fees more profitable to pools than a rising price? Let’s find out. Retrieved December 9, 2018, https://medium.com/@patrickob/are-transaction-fees-more-profitable-to-pools-than-block-rewards-lets-find-out-f65c92c538ec

ACKNOWLEDGEMENT

This work is funded by Fujitsu Ltd.