Time-dependent Decision-making and Decentralization in Proof-of-Work Cryptocurrencies

Yevhen Zolotavkin, Julian Garcia, Joseph Liu

CSF 2019
Main points of the paper

Without miners PoW consensus is impossible

What are the INCENTIVES and IMPACT of the miners?

INCENTIVES

MINER #1

Utility

“Where to mine?”

decision 1

INCENTIVE 1

IMPACT 1

On distribution of power

MINER #2

decision 2

INCENTIVE 2

IMPACT 2

Whole system

distribution

INCENTIVES

IMPACT 1

IMPACT 2

IMPACT n

Whole system

distribution

... in the details

IMPACTS

...
Incentives and their properties

1. Decision/action of a miner at every moment can be expressed using **utility**.

   - **Why?** Because pools use reward systems that encourage loyal and steady mining behavior.

3. Future is unknown. Miners must have **beliefs** to calculate utility and make decisions.
   - **Why?** Because it is important to know how (slow / fast) miners will be rewarded.

4. **Problems**: a) the space of beliefs is unknown; b) beliefs must be **consistent**.

   *Already defined in PROP, PPLNS, etc.*

   *Needs to be expressed in formal way – How?*
Future compensations
Utility for mining in a PPLNS pool → time discounting

What is more valuable: 1$ received today OR 1$ received tomorrow?

Is it applicable to PoW mining market?

1$ invested today generates profit in the future… similarly, 1$ invested tomorrow…

however, today investment outperforms tomorrow investment… therefore, today we should discount tomorrow reward…

and, hence, express time preference in monetary terms.
Investment opportunities for cryptocurrencies

BlockFi (https://blockfi.com/crypto-interest-account/)

For example, we can use exponential model to discount reward that is deferred $n$ days.

With 6.2% of annual yield we calculate parameter

$$k = \frac{\ln(1.062)}{365} \approx 1.65 \times 10^{-4}.$$

Further: we demonstrate that intensity of time discounting plays important role in decentralization of blockchain.
Settings and Limitations

The system consists of Pool #1 and Pool #2.

Limitations:

A. We consider a closed system of 2 pools.
B. We consider Pay Per Last N Shares (PPLNS) pools only.
C. Parameter $N$ is the same for the both pools.
Incentives and Decisions
Miners may move between the pools based on their best response

1. Calculate utilities to ‘stay’ and to ‘leave’ for each of the miners;
2. Make decision for each miner based on which utility is larger.

Is there a state of stability?
Equilibrium in the system

Assumption about personal beliefs allowed us to reason about utilities, best responses, and to demonstrate that equilibrium exists.

Brief conclusions:

A. Miners tend to leave the smaller pool.

B. Composition of the smaller pool and intensity of time discounting do matter.
The rest of the presentation

In order to understand effects of possible migration between the pools we are going to discuss:

- PoW mining in the pools
- PPLNS reward scheme
- Utility of the miners in PPLNS pools
- Simplifying assumptions about beliefs
- Algorithm to find equilibrium
- Simulation and discussion
Purpose of PoW mining: BitCoin

What is Bitcoin Mining?

It’s a decentralized computational process that serves 2 purposes:

1. Confirms transactions in a trustful manner when enough computational power (effort) is devoted to a block
2. Creates (issues) new bitcoins in each block

Bitcoin community awards miners with a standard reward (which is being halved every several years, now it is 12.5 BTC) plus 1.4 BTC on average collected from the fees of transactions included in the block.

Miners are incentivized by new coins but they have to follow the procedure.
Simplified procedure of block mining

Solving puzzle is the most computationally intense stage

Image source: www.weusecoins.com
A round of puzzle solving

Ability to organize parallel computations is the core reason for popularity of PoW mining pools.

Partial solutions are allowed in the pools and are called “shares”.

Why is that important for the miners?
Differences in mining power

Not all miners are equal. Mining difficulty is rising constantly…

As a result, smaller miners may experience significant income variance in case of solo mining.

Pools attract miners as they provide steady income (lower variance).
Pools are extremely important for the BitCoin network. Many of the reward systems calculate miners’ payoffs based on the distribution of their shares in time.

### Contribution of the pools to PoW mining

<table>
<thead>
<tr>
<th>Name</th>
<th>Reward Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>AntPool</td>
<td>PPLNS &amp; PPS</td>
</tr>
<tr>
<td>BTC.com</td>
<td>FPPS</td>
</tr>
<tr>
<td>BCGMonster.com</td>
<td>PPLNS</td>
</tr>
<tr>
<td>Jonny Bravo’s Mining Emporium</td>
<td>PPLNS</td>
</tr>
<tr>
<td>BitcoinAffiliateNetwork</td>
<td>?</td>
</tr>
<tr>
<td>Slush’s pool (mining.bitcoin.cz)</td>
<td>Score</td>
</tr>
<tr>
<td>BitMinter</td>
<td>PPLNSG</td>
</tr>
<tr>
<td>BTC.com</td>
<td>PPS</td>
</tr>
<tr>
<td>BTC.com</td>
<td>DGM</td>
</tr>
<tr>
<td>btcmp.com</td>
<td>PPS</td>
</tr>
<tr>
<td>BW Mining</td>
<td>PPLNS &amp; PPS</td>
</tr>
<tr>
<td>Eclipse Mining Consortium</td>
<td>DGM &amp; PPS</td>
</tr>
<tr>
<td>Effii</td>
<td>CPPSRB</td>
</tr>
<tr>
<td>F2Pool</td>
<td>PPS</td>
</tr>
<tr>
<td>GHash.IO</td>
<td>PPLNS</td>
</tr>
<tr>
<td>Give Me COINS</td>
<td>PPLNS</td>
</tr>
<tr>
<td>KanoPool</td>
<td>PPLNS</td>
</tr>
<tr>
<td>Merge Mining Pool</td>
<td>DGM</td>
</tr>
<tr>
<td>P2Pool</td>
<td>PPLNS</td>
</tr>
<tr>
<td>PotMine</td>
<td>SMPPS</td>
</tr>
<tr>
<td>MergeMining</td>
<td></td>
</tr>
</tbody>
</table>

PPLNS is the most popular reward scheme in the pools.
Reward principle of PPLNS

Miners share reward from the full solution in proportions to the numbers of shares that each of them submitted among the most recent N shares.

For example, on this scheme we can see that the latest reward is ought to be divided among N=20 shares where 8 shares were submitted by miner A and 12 shares were submitted by miner B. In “stable mining”, in expectation, reward is proportional to the individual power of a miner.

However, in order to understand incentives to migrate we need to consider marginal utility of a miner from mining one more share in the pool. It will be demonstrated that N and the total power of the pool play important role.
Utility of *miner A* – continuous model (part 1)

Analogy between discrete and continuous models for mining in PPLNS pool

**Discrete**: Energy $\Delta E$ is spent on a share which is produced by either *miner A* or *miner B*.

**Continuous**: Each $\Delta E$ has a portion that is contributed by *miner A* as well as the portion contributed by *miner B*.

Miner A: 40% of power
Miner B: 60% of power

Probability to be rewarded

$$D = \frac{1}{E_N} \int_{t_0}^{t_0 + \frac{E_N}{P}} Pf(t - t_0) dt$$

Probability to reward

$$P(T|\Delta E) = \frac{P_A}{P} \Pr(B|\Delta E)$$
Utility of miner $A$ – continuous model (part 2)

Probability to find

Fraction of miner $A$’s

Probability that miner $A$ brings reward to the pool during $\Delta t$ is $\frac{P_A}{P} \Pr(\mathbb{B} | \Delta E)$.

If this does not happen, her contribution $\Delta E \frac{P_A}{P}$ will be rewarded in the future. This happens with probability $1 - \frac{P_A}{P} \Pr(\mathbb{B} | \Delta E)$.

Miner A: 40% of power
Miner B: 60% of power

Probability to reward $\frac{P_A}{P} \Pr(\mathbb{B} | \Delta E)$

Probability to be rewarded $(1 - \frac{P_A}{P} \Pr(\mathbb{B} | \Delta E))$

$D = \frac{1}{N} \sum_{i=1}^{N} \lambda(n_i)$
Utility of miner A – continuous model (part 3)

Among the past $N$ successes, miner A expects to reward

Thus, miner A expects to reward her past with $R \frac{P_A}{P} F_A \Pr(B|\Delta E)$, and to get rewarded in the future with

$$R \frac{P_A}{P} \Pr(B|\Delta E) \left(1 - \frac{P_A}{P} \Pr(B|\Delta E)\right) \mathcal{D},$$

where $\mathcal{D}$ is the coefficient of time-discounting for future compensations.

Miner A 40% of power
Miner B 60% of power

Therefore, miner A expects to reward
Decision of a miner in the system of two pools

For a system that consist of a single pool, util...

We introduce disjoint sets $M_1$ and $M_2$ to denote pool membership.

Decision logic: at $t_0$ miner selects the pool where her utility is larger. Denote $U_{i,1}$ and $U_{i,2}$ utilities of miner $i$ in pools #1 and #2, respectively. For simplicity, we use $\bar{U}_i, \bar{U}_j$ such that $\text{sgn}(\bar{U}_i) = \text{sgn}(U_{i,1} - U_{i,2})$ and $\text{sgn}(\bar{U}_j) = \text{sgn}(U_{j,1} - U_{j,2})$. We search for equilibrium:

$$\forall i, j \left( \left( i \in M_1 \right) \land (\bar{U}_i \geq 0) \lor \left( j \in M_2 \right) \land (\bar{U}_j \leq 0) \right).$$

Simplified utilities $\tilde{U}_i$ and $\tilde{U}_j$ are defined by

$$\tilde{U}_i = F_{i,1} + \mathcal{D},$$

where are the fractions of past contributions in #1 and #2, resp.

and, are time-discounting coefficients in #1 and #2, resp.

Time-discounting coefficients are affected by the moves of other miners who have beliefs about the future.
Assumptions, beliefs and their effects

System of beliefs:
1) Every miner makes at most 1 move;
2) Larger pool remains always larger.

Assumption: All the miners have identical beliefs about the fi

Proofs

Effects on the system: a) there is an equilibrium which is acr

How does this help in finding equilibrium?
We still need to analyze decisions of the other miners, but...

CONSISTENT

simplifies reasoning and computations
Time-discounting coefficients

Without the loss of generality, total mining power of 2 pools is 1.

Unknown mining power of pool #1, $P_1$, affects how fast a miners will be compensated. As a result, this influences time-discounting coefficients and we have:

$$D_{1,i} = \frac{1}{E_N} \int_{t_0}^{t_0+E_N/P_1} P_1 f(t-t_0) dt,$$
$$D_{2,i} = \frac{1}{E_N} \int_{t_0}^{t_0+E_N/(1-P_1+p_i)} (1-P_1+p_i) f(t-t_0) dt,$$
$$D_{1,j} = \frac{1}{E_N} \int_{t_0}^{t_0+E_N/(P_1+p_j)} (P_1+p_j) f(t-t_0) dt,$$
$$D_{2,j} = \frac{1}{E_N} \int_{t_0}^{t_0+E_N/(1-P_1)} (1-P_1) f(t-t_0) dt,$$

where $f(t-t_0)$ is the time-discounting function. For the exponential model we have:

$$f(t-t_0) = f(E-E_0) = e^{-\theta E E_0 / E_N}.$$
Properties of the model

Assumption that there is an equilibrium at some point $t^*, t^* \geq t_0$,

We improve computational efficiency if we take into account the following properties (proofs):

1) None of the miners from larger pool (pool #2) has an incentive to join smaller pool;

2) $\forall E', E'' (E'' \geq E' \geq E_0) \vdash (M_2^{E'} \subseteq M_2^{E''})$, e.g.

3) $\forall \theta \left( (\theta \leq 0.5) \vdash (\partial \tilde{u}_i \geq 0) \right)$, e.g. in pool #1, i

As a result, we can find equilibrium using
Algorithm to find equilibrium

\( P_1^* \) -- Total power of pool #1 pri

\( D = \{D_1, D_2, \ldots, D_n\} \) -- normal

\( \theta \) -- time-discounting factor;
Experimental results

Distribution of mining power inside ‘Kano’ pool

<table>
<thead>
<tr>
<th>Power range</th>
<th>Number of miners</th>
<th>Total power</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P_{min}$</td>
<td>$P_{max}$</td>
<td></td>
</tr>
<tr>
<td>$4.3 \times 10^{-8}$</td>
<td>0.0048</td>
<td>692</td>
</tr>
<tr>
<td>0.0053</td>
<td>0.0081</td>
<td>7</td>
</tr>
<tr>
<td>0.0102</td>
<td>0.015</td>
<td>4</td>
</tr>
<tr>
<td>0.0166</td>
<td>0.0185</td>
<td>2</td>
</tr>
<tr>
<td>0.0247</td>
<td>0.0247</td>
<td>1</td>
</tr>
<tr>
<td>0.0374</td>
<td>0.0374</td>
<td>1</td>
</tr>
<tr>
<td>0.0443</td>
<td>0.0443</td>
<td>1</td>
</tr>
<tr>
<td>0.0706</td>
<td>0.0706</td>
<td>1</td>
</tr>
<tr>
<td>0.1875</td>
<td>0.1875</td>
<td>1</td>
</tr>
<tr>
<td>0.2445</td>
<td>0.2445</td>
<td>1</td>
</tr>
</tbody>
</table>

Some medium/small pool

Example: with $\theta = 0.01$ a n

Is there a way to protect smaller pool?
Sufficient Individual Power (SIP)

Example: composing pool #1 out of miners with individual power greater than 3% of total system power would be sufficient to protect the pool in a quite competitive investment environment.

However, we need such $p_i$ to

This is expressed as:

What are the consequences for miners if SIP is not achieved?
Effects on cumulative utilities of different miners

We calculate the relative change

\[ Q_i = \frac{c_i}{c_{i-1}} \]

Observation: effects on cumulative utilities differ significantly for different miners!
Conclusions

1) A closed system of two PPLNS mining pools (with the same $N$) is considered;

2) We demonstrated that time-discounting is important for the decision ("which pool to join?") that miners make;

3) We made reasonable assumptions that limit the space of miners’ beliefs about the future;

4) For the process of miner migration (from the smaller pool to the larger one) we have:

5) Even for moderate $\theta$ common composition of the smaller pool can be:

6) We suggest two kinds of mitigation: a) compose pools with miners who satisfy Sufficient Individual Power (SIP) requirement; b) adjust parameter $N$ for each pool accordingly.
Thank you for your attention!