2019 IEEE 32nd Computer Security Foundations Symposium (CSF)

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

Yevhen Zolotavkin, Julian Garcia, Joseph K. Liu
Faculty of Information Technology
Monash University, Clayton
3800 Victoria, Australia
Email: yevhen.zolotavkin@monash.edu, julian.garcia@monash.edu, joseph.liu@monash.edu

***Abstract*—Pool mining is a common way to reduce income variance for miners in Proof of Work Cryptocurrencies. A vast majority of mining does happen in pools, where a popular scheme to distribute rewards is Pay per last N Shares (PPLNS). In PPLNS and related schemes, miners are frequently making decisions whose rewards are not immediate and will only manifest in the future. This implies that models of inter-temporal utility are relevant when considering the incentives of miners. We show that when including these features of human behaviour in models of rational pool miners, the conditions that lead to decentralisation are hampered because larger pools may be more attractive to miners. We present a new game theoretical model of PPLNS where rational miners have time preferences. In this setup, the incentives of miners to work for a pool depend on the initial distribution of power between mining pools, as well as the specific details of how time is discounted. Agents jumping to larger pools face a trade-off between reducing the expected payoff from their shares in their current pool, or getting faster rewards in the future by joining a larger pool. We consider a case where pools of different mining power have the same size of reward window N. According to our study, in equilibrium larger pools have a tendency to accumulate a disproportionate share of the network power at the expense of smaller pools. This outcome is prevalent over a large range of realistic model parameters. Our model shows that PPLNS may be harmful to the decentralised governance of cryptocurrencies. A way to ameliorate these negative effects, is to encourage pools to have diverse window sizes, or use different reward mechanisms. Doing this in a decentralised fashion is an open challenge.**

***Index Terms*—blockchain, pooled mining, game theory, time discounting**

I. Introduction

A variety of cryptocurrencies rely on the Proof-of-Work (PoW) principle, whereby consensus is reached solving costly computation puzzles [1]–[3]. Miners exchange computation for the chance to earn newly minted currency [4]. Solo mining entails a very large variance in expected monetary payoffs. Because miners prefer stable income across time, solo mining is rare. Instead, miners join pools, in which the benefits of newly found blocks are shared among the pool members, guaranteeing a stable and steadier compensation for mining. Pools have different compensation schemes, determining how effort translates into monetary payoffs [5], [6].

Pools have adopted a variety of reward schemes, including, Pay Per Share (PPS), Proportional reward (PROP) and Pay per Last N Shares (PPLNS). Historically, PPS and PROP where the first schemes implemented in bitcoin mining pools. With PPS, miners are immediately compensated for their mining which requires solving puzzles of a lower complexity which are called "shares". Upon submission, every share is rewarded by the pool manager in proportion to its complexity. On the other hand, the pool profits from a full block, randomly appearing among the shares. A strong disadvantage of PPS is that managers need to absorb the variance associated with finding full solutions. This is reflected by higher pool fees on miners [7].

In PROP pools, fees collected from miners are smaller. However, the rewards are distributed among the shares that were submitted during one round of mining and only when the full solution of the puzzle is found by that pool. As a result, the reward is distributed over a variable number of shares. Due to this, PROP is vulnerable to "pool hopping" attacks, in which rational miners increase their returns by switching their mining activity between different pools [8].

PPLNS promises to reduce the incentives for hopping [9] while retaining cheaper fees [7], [10]. It is therefore the most popular mining reward scheme in operation, and its main idea is to reward only N of the most recent shares preceding the full solution. This temporal dimension for rewards has strong implications in decision making, that as we will show, can ultimately increase centralisation in the network.

Mining decisions (e.g., how much power to allocate across pools, which pools to join, etc) have immediate costs (electricity, equipment) but deferred benefits (mining reward). Inter-temporal utility is accordingly an important factor to consider. Most rational decision-makers would prefer 100 dollars now than tomorrow, for a variety of reasons [11]. Thus we say, that rational decision makers discount the future. By how much, will depend on their time preferences. The standard model to capture this basic idea is *exponential discounting*. In case of discrete time registration (e.g. days) it is defined by a discount parameter $0 < \delta < 1$. Thus, a level of utility u is worth $u\delta$ tomorrow, $u\delta^2$ the day after tomorrow and so forth. Discounting is prevalent in decision-making models involving a time horizon, and has a wealth of empirical and theoretical support [12]. Our aim here is to introduce time preferences into models of rational miners, and to study its consequences.

Time preferences are known and documented in the decision making literature, and can be compounded by the investment nature of cryptocurrency mining. To see why consider the following example. It is common for PPLNS pools to charge 1% fee, while PPS pools charge 2%. In the case of a small

DOI 10.1109/CSF.2019.00015

PPLNS pool, a share submitted today will be fully compensated in 2 weeks (on average) [13], [14]. On the other hand, a PPS pool guarantees same-day compensation. If a miner decides to mine with PPS pool and immediately deposits her revenue for 14 days with 1.5% interest [15], she will obtain $0.98 \times 1.015 \approx 0.995$ value out of every share which is greater than the 0.99 corresponding to PPLNS. Thus, deferred rewards can only be compared with the immediate compensation when the appropriate discounting is applied. In the proposed example, this discount factor is $\delta = 1.015^{-\frac{1}{14}} \approx 0.9989$.

In addition to purely economical motivations, discounting the future has a broader appeal in technical terms. Pool hardware infrastructure – including central servers and network equipment – need to remain functional in the future in order to compensate current mining contribution of a miner. Reliability of this hardware, often expressed by Time to Failure (TTF), is exponentially distributed [16]. Likewise, regular and accurate payments to the miners require that pool accounts remain secure and protected from malicious cyber attacks. This security also deteriorates with a probability that is exponentially dependent on time [17]. Thus, the intrinsic features of the technical infrastructure add up to the importance of miners discounting their future rewards.

A. Related work

Questions related to mining decisions and their impact on blockchain decentralization have been previously discussed in the cybersecurity literature. In particular, a number of identified attacks directly concern centralization of mining power. These include *double spending* [1], [18]–[20], *block withholding* [8], [21], [22], *selfish mining* [7], [23] among others [4], [24], [25]. A number of desirable blockchain properties can be hampered due to incompatible mining incentives. Game theoretical models have been shown to be useful in mitigating these phenomena [26], [27].

While many factors have been studied, including network characteristics [5], reward systems [28], mechanisms to reduce payments variance [29] among others; it remains unclear why *compensation times* have attracted so little attention [10]. Here, we show that the time of compensation of individual mining contributions to the pool is an important tool. It is therefore necessary to take it into account to encourage a healthy ecosystem robust to the attacks described in the literature. We do this by studying the incentives of miners to migrate across mining pools.

B. Our contribution

We present a new game theoretical model that shows that miners with reasonable behavioral assumptions have incentives to migrate from smaller PPLNS pools to larger PPLNS pools. In order to understand migration incentives we study the trade-offs between leaving and staying in the initial pool, in the presence of other more powerful pool. This problem is tackled by applying standard exponential time discounting. We show the existence of a Nash equilibrium of the underlying game and propose an algorithm to efficiently compute this equilibrium.

We reason that different pools may offer different compensation speeds. This fact may play an important role for miners who seek to increase their short-term future income. On the other hand, computational effort that has already been contributed by the miners (in the past) in their initial pool, entitles them to certain compensation, according to PPLNS defined in that pool. In the case of leaving their initial pool, the rewards for the previous efforts will be received by the miners at a slower pace. Actions of other miners may dictate a specific action for each miner because the speed of compensation in each pool depends on the total power of all its miners. Our model demonstrates that even marginal differences in pool size are enough to incentivise small miners to seek larger pools. This process accelerates when pools have either a high proportion of small-power miners or higher time-preferences.

The process of migration from smaller to larger PPLNS pools induces a pool market dominated by a handful of very large pools – as observed in reality. This centralization of power, runs counter to the spirit of decentralized cryptocurrencies. Large pools getting larger and small pools getting smaller will ultimately lead to an environment prone harmful attacks [21], [22], [25]. Our model also suggests how this "aggregation" effect can mitigated.

The rest of this paper is organized as follows. A game-theoretical model for competition between PPLNS pools is presented in Section II. It describes our assumptions about individual beliefs and the distribution mining power in the future. Section III presents a novel method that finds equilibrium in the system with two PPLNS pools. We analyze different properties of the system including migration rate, long-term effect on the utilities of the miners, as well as a sufficient condition to prevent migration from the smaller pools. We also present experimental results and discuss their impact on the security of PoW blockchains are discussed in Section IV. We present conclusions in Section V.

II. A game-theoretical model of pool competition

A schematic representation of PPLNS on fig. 1 explains the principle behind the reward scheme for a window size $N = 20$ shares. Miners A and B have 40% and 60% of the power inside the pool, and receive proportional payments to their shares submitted in two overlapping windows of size N. Full solutions are not usually considered a valid share and are excluded from the count. For instance, the most recent payment is equally divided among 20 shares: 8 shares belong to miner A and 12 shares belong to miner B fig. 1. As a result, in this particular example, miners receive 40% and 60% of block reward, respectively (for simplicity, the mining fees are not taken into account). Further, we will analyze PPLNS on a more detailed level.

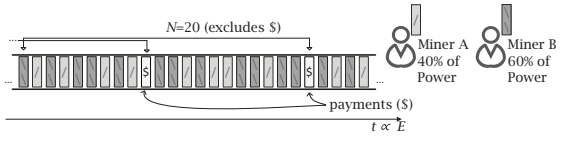

Figure 1: Rewards in PPLNS pool with two miners.

We consider a system of two PPLNS pools which is closed in the sense that nobody either joins nor leaves it. For

convenience, we regard a continuous model of mining where total mining power of the system is 1. In contrast to submission of shares at discrete moments, miners in our model prove their work by committing energy. They report personal consumption of (electrical) energy that is used for computations of PoW puzzle for a particular pool. We assume no network delays, computational equipment of all miners is equally efficient. Supposing that miners are never switching off their equipment, amount of computations delivered by every miner in each of the pools is determined by her computational power and pool membership. Continuous nature of our model simplifies reasoning about future rewards subject to time discounting.

The process of migration between the pools begins at moment t_0 and unfolds in time $t \in [t_0, \infty)$. An elementary portion of energy consumed by the system on computations during Δt is ΔE. The corresponding elementary contribution of miner i with individual power p_i is $\Delta t p_i = \Delta E p_i$. At every moment in the interval $[t_0, \infty)$ each miner finds the best allocation for her elementary contribution. The choice affects the reward chances for her past contributions in that pool (as a result of finding a full solution $\mathbb{B}$ of the puzzle). If this does not happen, her elementary contribution is expected to be rewarded in the future as a result of mining activity in that pool.

A. Preliminaries

We assume that every miner in the system is aware of the past and present moves of other miners. The decisions of all the miners at time t determine how mining power is distributed between the pools. In our model, $t \propto E$, hence we will express the quantities of interest as a function of E, instead of t (see table I for a list of variables and their meaning). These two views are equivalent, but we will focus on E for simplicity.

Let us discuss competition between pool #1 and pool #2. Each pool has PPLNS windows N_1 and N_2 measured as number of discrete shares. Because we work with a continuous model, these PPLNS windows are expressed as the corresponding amounts of mining energy, $E_{N,1}$ and $E_{N,2}$. A schematic picture of the setup is presented in fig. 2. The areas inside the large bars are used to denote energy consumed by computations in the corresponding pool. It also includes shaded areas that represent the contribution of miner i. The current elementary portion of effort $\Delta E p_i$ of miner i (small black rectangle) should be allocated at moment $E' \geq E_0$ to a pool that provides the best possible utility for that miner.

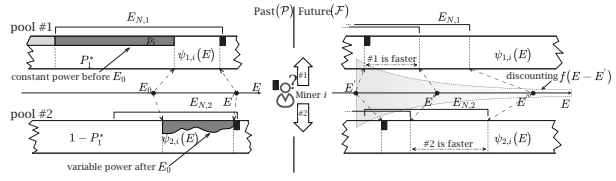

Figure 2: Response of miner i under specific beliefs and time discounting.

Prior to moment E_0 the composition of both pools is constant, with n miners whose membership to either pool #1 or pool #2. To denote pool membership we use $\mathbf{M}_1$ and $\mathbf{M}_2$; such that $i \in \mathbf{M}_1$ indicates miner i is in pool #1. We assume $\mathbf{M}_1 \cap \mathbf{M}_2 = \varnothing$. The total power of each pool is P_1^* and $1 - P_1^*$, respectively. Without loss of generality, we condier $P_1^* \leq 0.5$. Membership of the miners can change during the interval $[E_0, \infty)$ as a result of miners migrating across pools. In order to calculate her utility, a miner i should estimate possible monetary compensations associated with the past (index $\mathcal{P}$) and the future (index $\mathcal{F}$) performance of the system.

Table I: Main variables

Variable	Description
E	Total mining energy spent by both pools as for the moment t
E_0, t_0	The moment when competition between the pools begins
P_1^*, $1 - P_1^*$	Power of pool #1 and pool #2, resp., at $E < E_0$
p_i	Individual power of miner i
$F_{i,1}(E)$, $F_{i,2}(E)$	Past contribution of miner i to the pools #1 and #2, resp., at moment E
$\mathcal{D}_{1,i}(E)$, $\mathcal{D}_{2,i}(E)$	Estimation of miner i for the discounting coefficients in the pools #1 and #2, resp.
$\mathbf{M}_1, \mathbf{M}_2$	Sets of indices of miners, who work at $E < E_0$ for pool #1 and pool #2, resp.
$\mathbf{M}_1^{E'}, \mathbf{M}_2^{E'}$	Sets of indices of miners, who work at $E' \geq E_0$ for pool #1 and pool #2, resp.
N_1, N_2	Size (in numbers of shares) of the reward windows for pool #1 and #2, resp.
$E_{N,1}$, $E_{N,2}$	Size (amounts of energy) of the reward windows for pool #1 and #2, resp.
R	Monetary reward for mining block $\mathbb{B}$
$\psi_1(E)$, $\psi_2(E)$	Power of pool #1 and pool #2, respectively, at moment E
$\psi_{1,i}(E)$, $\psi_{2,i}(E)$	Individual estimation of miner i (using beliefs) for power of pool #1 and pool #2, respectively, at moment E
$\Psi_{1,i}$, $\Psi_{2,i}$	Individual constant estimation of miner i (using beliefs) for power of pool #1 and pool #2, respectively
Ψ_1, Ψ_2	Constant power of pool #1 and pool #2, respectively, in equilibrium at $E \geq E_0$
$f(E-E_0)$	Discounting that a miner makes at E_0 for the future reward collected at $E \geq E_0$
k	Parameter of exponential and discounting
θ	Discount coefficient such that $\theta = kE_{N,1}$
$b_i(E)$	Best response of miner i at moment E
$U_{i,1}(E)$, $U_{i,2}(E)$	Utilities of miner i at moment E for selecting pool #1 or #2, respectively
$\tilde{U}_i(E)$	Comparative utility (pool #1 vs #2) of miner i at moment E
$C_{i,1}$, $C_{i,2}$	Cumulative utilities of miner i for "stay" and "leave", resp.
$C_{i,1}^*$	Cumulative utility of miner $i \in \mathbf{M}_1$ for the "no competition – no move" mining scenario
Q_i	Indicator of relative change of cumulative utility of miner i

The past and future distribution of the power between the pools determines the incentives of miner i. The past distribution of mining power between the two pools, $\psi_1(E)$ and $\psi_2(E)$, $E \leq E'$, are unique and known to every miner. The future distribution is unknown, however, every miner i can estimate $\psi_{1,i}(E)$ and $\psi_{2,i}(E)$ for pool #1 and #2, respectively, $E \geq E'$, based on prior beliefs.

The importance of personal beliefs for the decisions that are made at E' can be illustrated with the following example. Suppose miner i expects that between moments E' and E'' pool #1 carries out more computations than pool #2, but expects the opposite in the interval E'' and E''' (see fig. 2). Other miners also have (potentially different) personal beliefs and make their choices between E' and E'''. The behavior of all the miners in the whole interval $E \in \left[E', E'''\right]$ defines the actual power of the

pools. The beliefs held by each miners can be assessed against evidence in the future. For some miners, the actual power of the pools at $E \in \left[E^{'}, E^{'''}\right]$, may contradict their initial beliefs. For instance, the described beliefs of miner i are not consistent if $\int_{E^{'}}^{E^{''}} \psi_1(E)\mathrm{d}E \leq \int_{E^{'}}^{E^{''}} \psi_2(E)\mathrm{d}E$ or $\int_{E^{''}}^{E^{'''}} \psi_1(E)\mathrm{d}E \geq \int_{E^{''}}^{E^{'''}} \psi_2(E)\mathrm{d}E$. In our approach, we only consider beliefs that are consistent for every miner at any moment $E \geq E_0$. This is not a stringent assumption, since we assume all players are rational.

Let us discuss utility and best response of miner i. We denote the response of miner i as $b_i(E)$ where $b_i(E) = 0$ indicates her choice of pool #1 and $b_i(E) = 1$ indicates of choice of pool #2. Then, the functions for the past distribution of power are defined as:

$$\psi_1(E) = \begin{cases} P_1^*, & \text{if } E < E_0; \\ \sum_{j=1}^{n} p_j\left(1 - b_j(E)\right), & \text{if } E \geq E_0; \end{cases}$$

$$\psi_2(E) = \begin{cases} 1 - P_1^*, & \text{if } E < E_0; \\ \sum_{j=1}^{n} p_j b_j(E), & \text{if } E \geq E_0. \end{cases}$$

The utility for selecting pool #1 will be denoted $U_{i,1}\left(E^{'}\right)$. Similarly, $U_{i,2}\left(E^{'}\right)$ will denote the utility for selecting pool #2. These utilities should account for components related to the past and future of the system (see fig. 2).

Let us start by discussing the past. The immediate effort $p_i\Delta E$ of miner i that is produced at $E^{'}$ rewards her past contribution only if she discovers full solution. This will happen with probability $p_i\mathrm{Pr}\left(\mathbb{B}\,\middle|\,\Delta E\right)$, where $\mathrm{Pr}\left(\mathbb{B}\,\middle|\,\Delta E\right)$ is the chance of finding a full solution $\mathbb{B}$ by spending energy ΔE. As a result of this, the pool of her choice will be rewarded with a monetary value R. The components for past rewards are:

$$U_{i,1}^{\mathcal{P}}\left(E^{'}\right) = Rp_i\mathrm{Pr}\left(\mathbb{B}\,\middle|\,\Delta E\right)F_{i,1}\left(E^{'}\right),$$

$$U_{i,2}^{\mathcal{P}}\left(E^{'}\right) = Rp_i\mathrm{Pr}\left(\mathbb{B}\,\middle|\,\Delta E\right)F_{i,2}\left(E^{'}\right).$$

Here, the parameters $F_{i,1}\left(E^{'}\right)$ and $F_{i,2}\left(E^{'}\right)$ indicate cumulative effort of the miner relatively to the total computational effort in each pool. These parameters are calculated using information from the most recent PPLNS windows of size $E_{N,1}$ and $E_{N,2}$, respectively.

The values of parameters $F_{i,1}\left(E^{'}\right)$ and $F_{i,2}\left(E^{'}\right)$ are determined by $\psi_1(E)$, $\psi_2(E)$, and $b_i(E)$, fig. 3. We will calculate $F_{i,1}\left(E^{'}\right)$ and $F_{i,2}\left(E^{'}\right)$ using intervals $\left[\check{E}_1, \hat{E}_1\right]$ and $\left[\check{E}_2, \hat{E}_2\right]$ for pool #1 and pool #2, respectively. The upper interval bounds are defined such that $\exists l \leq n\left(b_l(\hat{E}_1) = 0,\ \hat{E}_1 \leq E^{'}\right)$ and $\exists m \leq n\left(b_m(\hat{E}_2) = 1,\ \hat{E}_2 \leq E^{'}\right)$ but $\nexists l \leq n\left(b_l(E) = 0,\ E > \hat{E}_1\right)$ and $\nexists m \leq n\left(b_m(E) = 1,\ E > \hat{E}_2\right)$. For example, in the diagram for the calculation of $F_{i,1}\left(E^{'}\right)$ and $F_{i,2}\left(E^{'}\right)$ on fig. 3 the right endpoints for both pools coincide with the current moment $E^{'}$. In general, it is required that at least one of them coincides with $E^{'}$. The lower interval bounds are defined such that $\int_{\check{E}_1}^{\hat{E}_1} \psi_1(E)\mathrm{d}E = E_{N,1}$ and $\int_{\check{E}_2}^{\hat{E}_2} \psi_2(E)\mathrm{d}E = E_{N,2}$. Fractional contributions of miner i to pools #1 and #2 are computed as

$$\begin{aligned} F_{i,1}\left(E^{'}\right) &= \frac{1}{E_{N,1}} \int_{\check{E}_1}^{\hat{E}_1} p_i\left(1 - b_i(E)\right)\mathrm{d}E, \\ F_{i,2}\left(E^{'}\right) &= \frac{1}{E_{N,2}} \int_{\check{E}_2}^{\hat{E}_2} p_i b_i(E)\mathrm{d}E\,. \end{aligned} \tag{1}$$

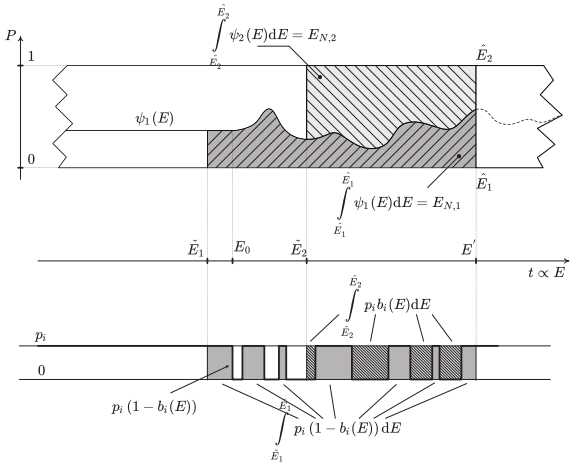

Figure 3: Calculation of past contribution of miner i in both pools at moment $E^{'}$.

If miner i is not successful in finding a full solution $\mathbb{B}$ for the chosen pool at moment $E^{'}$, her elementary contribution $p_i\Delta E$ will be rewarded in the future. This will happen with probability $1 - p_i\mathrm{Pr}\left(\mathbb{B}\,\middle|\,\Delta E\right)$. The monetary value of her contribution $Rp_i\mathrm{Pr}\left(\mathbb{B}\,\middle|\,\Delta E\right)$ will be reimbursed throughout some time which duration may be different for each pool. Rational agents valuate reward paid in such form at a level which is lower compared to the equivalent monetary value that is payed instantly. The corresponding coefficients that discount monetary reward of miner i at moment $E^{'}$ will be denoted as $\mathcal{D}_{1,i}(E^{'})$ and $\mathcal{D}_{2,i}(E^{'})$ for pool #1 and pool #2, respectively. Therefore, for miner i, components of total utilities that are associated with future performance of corresponding pool can be expressed as

$$U_{i,1}^{\mathcal{F}}\left(E^{'}\right) = \left(1 - p_i\mathrm{Pr}\left(\mathbb{B}\,\middle|\,\Delta E\right)\right)Rp_i\mathrm{Pr}\left(\mathbb{B}\,\middle|\,\Delta E\right)\mathcal{D}_{1,i}(E^{'}),$$

$$U_{i,2}^{\mathcal{F}}\left(E^{'}\right) = \left(1 - p_i\mathrm{Pr}\left(\mathbb{B}\,\middle|\,\Delta E\right)\right)Rp_i\mathrm{Pr}\left(\mathbb{B}\,\middle|\,\Delta E\right)\mathcal{D}_{2,i}(E^{'}).$$

Let us express discount coefficients $\mathcal{D}_{1,i}(E^{'})$ and $\mathcal{D}_{2,i}(E^{'})$. Their values depend on the speed of future compensation. This is reflected by discounting function $f(E - E^{'}) \in (0, 1)$ which is decreasing in $E \geq E^{'}$. A new influx of ΔE energy into the system at E implies that $\psi_{1,i}(E)\Delta E$ is consumed by pool #1. In expectation, this mining activity induces compensation that is $\frac{\psi_{1,i}(E)\Delta E}{E_{N,1}}$ in proportion to the total monetary reward, $Rp_i\mathrm{Pr}\left(\mathbb{B}\,\middle|\,\Delta E\right)$, for miner i. Her contribution made at $E^{'}$ is

eligible for payments as long as it is within the most recent portion $E_{N,1}$. We denote $\grave{E}_1$ the moment when cumulative amount of energy that has been used by pool #1 since $E^{'}$ equals to $E_{N,1}$. Therefore, discount coefficients for miner i at moment $E^{'}$ are calculated as

$$\begin{aligned}\mathcal{D}_{1,i}(E^{'}) &= \frac{1}{E_{N,1}} \int_{E^{'}}^{\grave{E}_1} \psi_{1,i}(E) f(E - E^{'}) \mathrm{d}E\,, \\ \mathcal{D}_{2,i}(E^{'}) &= \frac{1}{E_{N,2}} \int_{E^{'}}^{\grave{E}_2} \psi_{2,i}(E) f(E - E^{'}) \mathrm{d}E\,,\end{aligned} \tag{2}$$

where $\int_{E^{'}}^{\grave{E}_1} \psi_{1,i}(E)\mathrm{d}E = E_{N,1}$ and $\int_{E^{'}}^{\grave{E}_2} \psi_{2,i}(E)\mathrm{d}E = E_{N,2}$ for pool #1 and pool #2, respectively.

Complete utilities for selecting pool #1 and pool #2 are $U_{i,1}\left(E^{'}\right) = U^{\mathcal{P}}_{i,1}\left(E^{'}\right) + U^{\mathcal{F}}_{i,1}\left(E^{'}\right)$ and $U_{i,2}\left(E^{'}\right) = U^{\mathcal{P}}_{i,2}\left(E^{'}\right) + U^{\mathcal{F}}_{i,2}\left(E^{'}\right)$, respectively. Substituting the corresponding expressions for the utilities for the past and the future, we obtain

$$U_{i,1}\left(E^{'}\right) = Rp_i \Pr\left(\mathbb{B}\,\middle|\,\Delta E\right)\left(F_{i,1}\left(E^{'}\right) + \left(1 - p_i \Pr\left(\mathbb{B}\,\middle|\,\Delta E\right)\right)\mathcal{D}_{1,i}(E^{'})\right),$$

$$U_{i,2}\left(E^{'}\right) = Rp_i \Pr\left(\mathbb{B}\,\middle|\,\Delta E\right)\left(F_{i,2}\left(E^{'}\right) + \left(1 - p_i \Pr\left(\mathbb{B}\,\middle|\,\Delta E\right)\right)\mathcal{D}_{2,i}(E^{'})\right).$$

In order to play a best response at $E^{'}$, miner i should select the pool yielding greater utility. Hence, the sign of the expression $U_{i,1}\left(E^{'}\right) - U_{i,2}\left(E^{'}\right)$ determines best response $b_i\left(E^{'}\right)$. Further we will use comparative utility $\tilde{U}_i\left(E^{'}\right)$ such that

$$U_{i,1}\left(E^{'}\right) - U_{i,2}\left(E^{'}\right) = Rp_i \Pr\left(\mathbb{B}\,\middle|\,\Delta E\right)\tilde{U}_i\left(E^{'}\right).$$

Taking into account that $Rp_i \Pr\left(\mathbb{B}\,\middle|\,\Delta E\right)$ is non-negative we arrive to

$$\operatorname{sgn}\left(U_{i,1}(E^{'}) - U_{i,2}(E^{'})\right) = \operatorname{sgn}\left(\tilde{U}_i(E^{'})\right),$$

where $\operatorname{sgn}(\cdot)$ is the signum function.

We use that $\lim_{\Delta E \to 0}\left[1 - p_i \Pr\left(\mathbb{B}\,\middle|\,\Delta E\right)\right] = 1$ to obtain:

$$\tilde{U}_i\left(E^{'}\right) = F_{i,1}\left(E^{'}\right) + \mathcal{D}_{1,i}(E^{'}) - F_{i,2}\left(E^{'}\right) - \mathcal{D}_{2,i}(E^{'})\,, \tag{3}$$

which represents incentives of miner i. The best response is

$$b_i\left(E^{'}\right) = \begin{cases} 0, & \text{if } \tilde{U}_i\left(E^{'}\right) \geq 0; \\ 1, & \text{if } \tilde{U}_i\left(E^{'}\right) < 0. \end{cases} \tag{4}$$

Future compensations entail more elaborate calculations for $\tilde{U}_i\left(E^{'}\right)$. Unlike $\psi_1(E)$ and $\psi_2(E)$, the functions $\psi_{1,i}(E)$ and $\psi_{2,i}(E)$ represent the estimates of miner i only. In the future, these individual estimations (or indirect beliefs about them) can be verified because functions $\psi_1(E)$ and $\psi_2(E)$ will be updated based on the known best responses of all miners. As expressed before, we will assume consistent beliefs at any $E \geq E_0$.

We proceed as follows. Lemma 1 and Lemma 2 deal with the consistency of specific beliefs, allowing us to state that there is a Nash equilibrium and it is reached at moment E_0. In order to define all the possible configurations of equilibrium we will consider a special case of our model of miners' incentives where $E^{'} = E_0$. For time discounting we will use the exponential function, as is often standard in models with discounting. Based on the properties of this discounting model, an efficient algorithm for equilibrium search will be developed and its complexity will be estimated. Finally, in the experiment section, we will analyze influence of several parameters of the system including initial distribution of mining power in the pools and the degree of time preference on the characteristics of equilibrium as well as its consequences for miners.

B. Payoff function with consistent beliefs

We will focus on the case when $E_{N,1} = E_{N,2}$, with specific beliefs about the values of $\psi_{1,i}(E)$ and $\psi_{2,i}(E)$ that will be shown to be consistent. We will focus for now on pure strategy Nash equilibria and how to find it. N may vary for different pools, however, as general rule $N = kD$ where D expresses current puzzle complexity over the average number of required shares, and k is usually a small integer number (e.g. 1, 2 or 5). This convention among pool administrators causes many different pools to have same value of N. In some cases, this number remains constant for a pool during long period of time due to the conservative attitudes of pool miners who oppose frequent changes [13], [14]. Next, we will introduce game-theoretical settings and definitions that will be applied to our model.

The process of migration of miners between the pools will be studied in the context of game-theoretical framework. Due to the continuous nature of the mining model, the game between the pools is an infinitely repeated game. The game begins at the moment t_0 and progresses through time t. For the closed system, there is an equivalence between time and total energy that is spent on computations by the both pools. Therefore, notations E_0 and E will be used to designate corresponding moments.

At any moment $E \geq E_0$, the strategy of miner i will be encoded using set $S = \{0, 1\}$. Different moves of miner i, $s_i = 0$ and $s_i = 1$ indicate mining in pool #1 and pool #2, respectively. Strategy profile at moment $E \geq E_0$ is a vector $\mathbf{s}^E = \{s_i^E\}_{i=1}^n$, $\mathbf{s}^E \in S^n$. We will use $\mathbf{s}^E_{-i} = \{s_j^E\}_{\substack{j=1 \\ j \neq i}}^n$ to denote strategy profile that excludes move of miner i.

Definition 1. *For miner i observing strategy profile $\mathbf{s}^{E^{'}}_{-i}$ at moment $E^{'} \geq E_0$ beliefs about the distribution of mining power (between the pools #1 and #2, respectively) in the future, at $E \geq E^{'}$, are represented by functions $\psi_{1,-i}(E)$ and $\psi_{2,-i}(E)$:*

$$\psi_{1,-i}(E) = \sum_{j=1, j\neq i}^{n} \left(1 - s_j^{E^{'}}\right) p_j, \quad \psi_{2,-i}(E) = \sum_{j=1, j\neq i}^{n} s_j^{E^{'}} p_j\,.$$

To discuss the incentives of miner i, we use functions $\psi_{1,i}(E) = \psi_{1,-i}(E) + p_i$, and $\psi_{2,i}(E) = \psi_{2,-i}(E) + p_i$. For any $E^{'} \geq E_0$ utility of miner i is a function $U_i\left(E^{'}, s_i^{E^{'}}, \mathbf{s}^{E^{'}}_{-i}\right) : E^{'} \times S^n \to \mathbb{R}$.

Definition 2. *Best response of miner i at moment $E' \geq E_0$ is represented using function $b_i\left(E', \mathbf{s}_{-i}^{E'}\right) : E' \times S^{n-1} \to \{0, 1\}$, such that $U_i\left(E', b_i\left(E', \mathbf{s}_{-i}^{E'}\right), \mathbf{s}_{-i}^{E'}\right) \geq U_i\left(E', 1 - b_i\left(E', \mathbf{s}_{-i}^{E'}\right), \mathbf{s}_{-i}^{E'}\right)$.*

We simplify the notation, by using $b_i(E') = b_i\left(E', \mathbf{b}_{-i}^{E'}\right)$, $\tilde{U}_i(E') \propto U_{i,1}(E') - U_{i,2}(E')$, where $U_{i,1}(E') = U_i\left(E', 0, \mathbf{b}_{-i}^{E'}\right)$, $U_{i,2}(E') = U_i\left(E', 1, \mathbf{b}_{-i}^{E'}\right)$ under assumption that prior to moment E_0 the distribution of mining power between the pools is such that $\forall j \in \mathbf{M}_2\left(P_1^* + p_j < 0.5\right)$. It will be demonstrated that given assumption is sufficient to guarantee at least one Nash equilibrium at $E \geq E_0$ with a profile $\mathbf{b}^{E_0}$. Some intuition about the equilibrium can be gained from the fact that for every member of the larger pool, best response is to remain in it.

Remark 1. *[Larger pool discounts less] We consider 2 pools for which mining power is expressed with the functions $\psi'(E)$ and $\psi''(E)$ for pool #1 and pool #2, respectively.*

$$\forall E \geq E_0\left(\psi''(E) \geq \psi'(E) \geq 0\right) \wedge \left(\int_{E_0}^{E''} \psi'(E)\,\mathrm{d}E = \int_{E_0}^{E'} \psi''(E)\,\mathrm{d}E\right) \vdash$$
$$\vdash \int_{E_0}^{E'} f(E - E_0)\psi''(E)\,\mathrm{d}E \geq \int_{E_0}^{E''} f(E - E_0)\psi'(E)\,\mathrm{d}E$$

if the discounting function $f(E - E_0) \geq 0$ is monotonically decreasing on $E \in [E_0, \infty)$. (See section A)

Based on the result of remark 1 we can reason that condition $\forall j \in \mathbf{M}_2\left(P_1^* + p_j < 0.5\right)$ prevents miners in $\mathbf{M}_2$ from joining pool #1. This allows us to restrict the study of incentives of switching between the pools (at different moments in time) to the set $\mathbf{M}_1$ of miners only. Next, we present results from lemma 1 and lemma 2 and discuss them in the context of Perfect Subgame Equilibrium (PSE) at every instance $E' \geq E_0$ of the game (for the proof see section B). We adopt notations $\mathbf{M}_1^{E'}$ and $\mathbf{M}_2^{E'}$ to refer to the set of all miners working at E' for pool #1 and pool #2, respectively (see table I).

Lemma 1. *$\forall E', E''$ if $\left(\forall j \in \mathbf{M}_2\left(P_1^* + p_j < 0.5\right) \wedge \left(E'' \geq E' \geq E_0\right)\right)$ then $\mathbf{M}_2^{E'} \subseteq \mathbf{M}_2^{E''}$.*

The fact that no miner ever leaves pool #2 guarantees that there is an equilibrium. The moment when equilibrium is achieved depends solely on the actions of miners from pool #1. Next, we will point out that if a miner leaves pool #1, her dominant strategy is to do so at E_0.[1] (for the proof see section B).

Lemma 2. *$\forall E'$ if $\left(\forall j \in \mathbf{M}_2\left(P_1^* + p_j < 0.5\right) \wedge \left(E' \geq E_0\right)\right)$ then $\mathbf{M}_1^{E_0} \subseteq \mathbf{M}_1^{E'}$.*

As a result, neither set $\mathbf{M}_1^E$ nor set $\mathbf{M}_2^E$ ever lose their elements on (E_0, ∞) and PSE is guaranteed. Another important conclusion about results of lemma 1 and lemma 2 is that $\psi_{1,i}(E)$ and $\psi_{2,i}(E)$ are indeed constants on (E_0, ∞) which connotates that assumption about the future expressed in definition 1 is correct. Further in the paper, estimations of miner i about future power for pool #1 and pool #2 will be referred as $\Psi_{1,i}$ and $\Psi_{2,i}$, respectively.

Lastly, soundness of the results requires validity of premise $\forall j \in \mathbf{M}_2\left(P_1^* + p_j < 0.5\right)$. Nevertheless, given condition is sufficient, but not necessary to reach an equilibrium at E_0. Besides that, cases with near equal mining power of two random PPLNS pools are quite rare. This supports soundness on practice.

We aim at analyzing possible profiles of equilibrium and discuss consequences for the community of PoW miners including questions of decentralization of corresponding blockchains. This requires algorithm that is computationally efficient for the pools with large number of miners. The task demands a closer investigation of properties of utility functions that may include different time-discounting models.

Let us reason about properties of the mining utility. For each miner, strategy profile consists of two possible actions, which in case of brute-force approach to the search of equilibrium would require 2^n operations. Therefore, even for pools with a moderate number of miners, brute-force search for equilibrium is not feasible. Here we discuss on how results of lemma 1, lemma 2 and properties of utility functions can be used to design a more efficient algorithm to find equilibrium at E_0.

We will discuss properties of miner utilities that are dependent on selection of discounting function $f(E - E_0)$. Exponential discounting function is one of the most popular [12]. It is defined as $f(E - E_0) = e^{-k(E-E_0)}$, where k specifies intensity of time discounting. We substitute parameters k with expression $k = \frac{\theta}{E_N}$, $\theta \geq 0$. For instance, for the monetary reward obtained at $E = E_0 + E_N$ discount factor is $e^{-\theta}$.

Results of lemma 1 suggest that miners who leave pool #1 never return back. Assuming there are $n_1 = \left|\mathbf{M}_1\right|$ miners prior to moment E_0, we re-initiate the procedure that searchers for a new candidate to leave the pool among the remaining miners. Maximum number of operations in that case is $\sum_{i=1}^{n_1} i = 0.5n(n-1)$ which corresponds to $O(n^2)$. Further, we will address property that will allow to reduce complexity to $O(n)$ for the case when information about power of miners is in the form of a sorted array.

Let us analyze utility of miner i. According to eqs. (1) and (2), $F_{i,1}(E_0) = \frac{p_i}{P_1^*}$, $F_{i,2}(E_0) = 0$, $\mathcal{D}_{1,i}(E_0) = \frac{\Psi_{1,i}}{E_N} \int_{E_0}^{E_0 + \frac{E_N}{\Psi_{1,i}}} f(E - E_0)\mathrm{d}E$, $\mathcal{D}_{2,i}(E_0) = \frac{\Psi_{2,i}}{E_N} \int_{E_0}^{E_0 + \frac{E_N}{\Psi_{2,i}}} f(E - E_0)\mathrm{d}E$. According to eq. (3), utility that is using exponential discounting function has expression of

$$\begin{aligned}\tilde{U}_i(E_0) =& \frac{p_i}{P_1^*} + \frac{\Psi_{1,i}}{E_N} \int_{E_0}^{E_0 + \frac{E_N}{\Psi_{1,i}}} e^{-\theta\frac{(E-E_0)}{E_N}}\mathrm{d}E - \\ &- \frac{\Psi_{2,i}}{E_N} \int_{E_0}^{E_0 + \frac{E_N}{\Psi_{2,i}}} e^{-\theta\frac{(E-E_0)}{E_N}}\mathrm{d}E = \\ =& \frac{p_i}{P_1^*} + \frac{\Psi_{1,i}}{\theta}\left(1 - e^{-\frac{\theta}{\Psi_{1,i}}}\right) - \frac{\Psi_{2,i}}{\theta}\left(1 - e^{-\frac{\theta}{\Psi_{2,i}}}\right).\end{aligned} \tag{5}$$

[1] Meaning of notation $\mathbf{M}_1$ should be distinguished from the meaning of $\mathbf{M}_1^{E_0}$ where the first specifies miners in pool #1 prior to E_0, while the second defines miners who are mining for pool #1 at E_0.

The following results will allow to reduce the number of computations and to discuss conditions when none of the miners in pool #1 has incentive to join pool #2. Their proofs (see section C) use some of the results from lemmas 1 and 2.

Corollary 1. *Under exponential discounting,* $\forall \Psi_{1,i}$, $\forall \theta \leq 0.5 \left(\partial \frac{\tilde{U}_i(E_0)}{\partial p_i} \geq 0\right)$.

Domain $\theta \in [0, 0.5]$ is sufficient to represent intensity of time discounting for the majority of rational miners. Higher values of discount parameters are associated with extremely impatient miners. For example, in case $\theta = 0.5$, a miner at E_0 should valuate the reward that she will obtain at $E_0 + E_N$ as $e^{-0.5} \approx 61\%$.

The presented outcomes indicate that miners with smaller power p_i have greater incentive to leave pool #1. Using results of lemmas 1 and 2 as well as corollary 1 we will design an efficient method to find pure strategy Nash equilibrium which is suitable in the context of the proposed discounting function. We will also question sufficient individual power to stay in pool #1.

III. Method, Equilibrium and its characteristics

A. Method to find equilibrium

The method to find Nash equilibrium between two PPLNS pools can be described as (fig. 4):

1) Sort the indices of all the miners in pool #1 in ascending order according to their power, so that $\forall i, p_i \geq p_1$;
2) Execute $|\mathbf{M}_1|$ steps of the algorithm. On step i of the algorithm, verify the incentive to leave (e.g. if $\tilde{U}_i < 0$ is true) for the miner with power p_i and $\Psi_{1,i} = P_1^* - \sum_{l=1}^{i-1} p_l$, record her decision as best response b_i. After step $|\mathbf{M}_1|$, return vector $\mathbf{b}$.
3) Analyze if $\mathbf{b}$ is either: i) "all 0"; ii) "all 1"; iii) contains '0' and '1'. In the cases i) and ii) there is only one possible equilibrium which is "all stay in pool #1" and "all leave pool #1", respectively. However, in case iii) there may be more than one equilibrium.

Table II: Distribution of mining power (normalized) in Kano pool

Power range		Number of miners	Total power
$p_{\min}$	$p_{\max}$		
4.3×10^{-8}	0.0048	692	26.29%
0.0053	0.0081	7	4.36%
0.0102	0.015	4	4.93%
0.0166	0.0185	2	3.51%
0.0247	0.0247	1	2.47%
0.0374	0.0374	1	3.74%
0.0443	0.0443	1	4.43%
0.0706	0.0706	1	7.06%
0.1875	0.1875	1	18.75%
0.2445	0.2445	1	24.45%

B. Experimental evaluation of equilibrium between two PPLNS pools

The resulting size of pool #1, Ψ_1, depends on the initial power P_1^*, distribution, and discounting. With the aim to estimate the severity of changes caused by miners leaving the pool, we run computer simulation. Data about distribution of mining power was collected from Kano pool, which

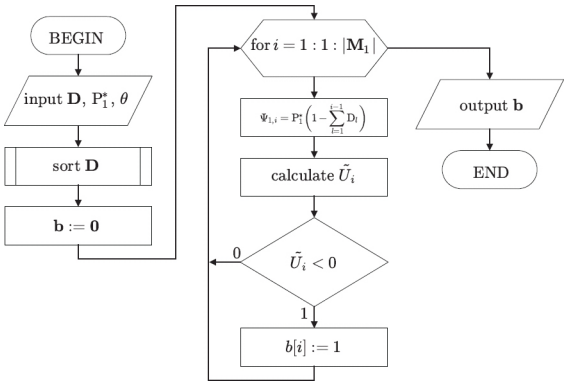

Figure 4: Diagram for the method to find equilibrium. Distribution $\mathbf{D}$ is obtained from Kano pool, normalized set, $\sum_{\mathbf{D}} D_l = 1$.

incorporates 711 miners table II. As it can be seen from the table, according to individual mining power of the miners, their distribution is significantly skewed. The data is normalized (total mining power sums to 1) and is denoted as $\mathbf{D}$ on the diagram fig. 4. Despite the fact that many equilibria are possible, on practice outcomes with more than one equilibrium were rare and occurred for $P_1^* \approx 0.5$.

Exponential discounting function was used for the experiment, with $0 < P_1^* < 0.5$, $\theta \in (0, 0.1]$. Fraction of mining power that is fleeing pool #1 in equilibrium was calculated and is depicted on fig. 5. It can be seen from there that the fraction is quickly increasing with θ, and, decreasing with P_1^*. On the both plots, there are noticeably large areas of a single color, meaning that the fleeing fraction remains stable even if P_1^* decreases and θ increases. This can be explained by highly disproportional power distribution inside the pools on practice, where vast majority are small miners, and few miners have significant power. In that regard, an important question to ask is the minimum power requirement that can provide resistance to pool migration. Such condition may be sufficient for decentralized PoW mining.

C. Sufficient individual power for incentive compatible mining in pool #1

We question the lower limit for individual power that guaranties incentive compatible mining in pool #1 for a miner in that pool. According to corollary 1, that condition is sufficient for more powerful miners to stay in pool #1, too. The value of sufficient individual power (SIP) is dictated by initial power of pool #1, P_1^*, and discount parameter θ . The latter is an intrinsic characteristic of miners' valuations and do not change over time. However, P_1^* may change if new miners join the pool, or current miners leave due to the reasons other than migration to pool #2. In order to provide practical recommendations for SIP, we remove previously agreed constraints of a closed system of two PPLNS pools. Since P_1^* may change its exact value is unknown. We consider the worst case scenario for that parameter. We plot SIP as empirical dependencies $\mathcal{S}(\theta)$, (fig. 6):

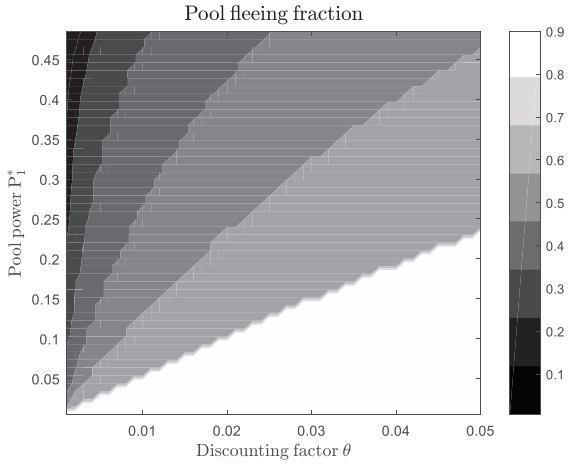

Figure 5: Fraction of the mining power of pool #1 that is fleeing to pool #2 under given θ and P_1^*.

$$\mathcal{S}(\theta) = \max_{P_1^*} \min_{\{\tilde{U}_1 \geq 0 \,|\, \theta, P_1^*\}} p_1 = \max_{\{P_1^* | \tilde{U}_1 = 0, \theta\}} p_1,$$

where $P_1^* \in [2p_1, 0.5)$ which is explained by the fact that a pool should have at least two miners with SIP. For instance, a practical recommendation that can be retrieved from the graphs for discount factor at 0.1 is to compose pool #1 from the miners which power is larger than 3% of the total power (of both pools).

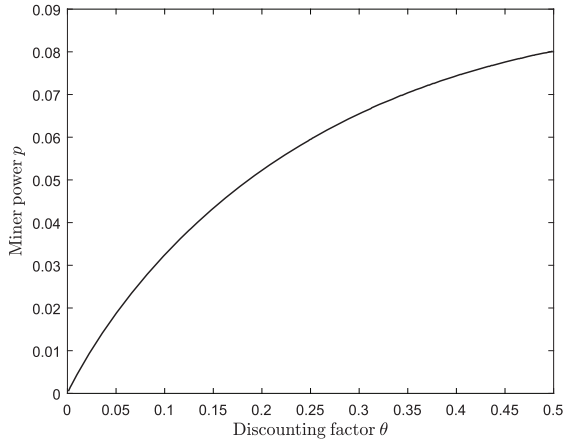

Figure 6: Sufficient individual power (SIP) for incentive compatible mining in pool #1.

D. Effect of equilibrium on cumulative utility of miners from pool #1

In case when requirement for SIP is not satisfied miners may leave pool #1. Migration of miners from pool #1 to pool #2 affects their long-term valuations. Miners from pool #2 are in a more advantageous position as they never abandon their pool, their individual past contributions are always rewarded, and, total power of their pool increases which according to remark 1 guarantees better valuations for the future rewards. On the other hand, miners from pool #1 may suffer losses. We express relative change in long-term expectations of these miners.

For each miner i from pool #1 we calculate her cumulative utility, $C_{i,1}$ or $C_{i,2}$ for $b_i(E_0) = 0$ or $b_i(E_0) = 1$, respectively, see section D. The utility is calculated over $E \in [E_0, \infty]$ and is defined by parameters P_1^* and θ, equilibrium profile, total power Ψ_1 of pool #1, individual mining power p_i. This is further compared with the cumulative utility $C_{i,1}^*$ of miner i for the hypothetical case when no miner leaves pool #1, $\Psi_1 = P_1^*$.

The indicator of relative changes in cumulative utility is determined as

$$Q_i = \begin{cases} \dfrac{C_{i,1} - C_{i,1}^*}{C_{i,1}^*}, & \text{if } b_i(E_0) = 0; \\ \dfrac{C_{i,2} - C_{i,1}^*}{C_{i,1}^*}, & \text{if } b_i(E_0) = 1. \end{cases}$$

Value of Q_i was computed for every miner in pool #1, with θ and θ^* taking values from diapason $[0, 0.1]$. The indices were assigned to the miners sorted in ascending order, according to their power, e.g. $\forall i, p_i \geq p_1$, see fig. 7.

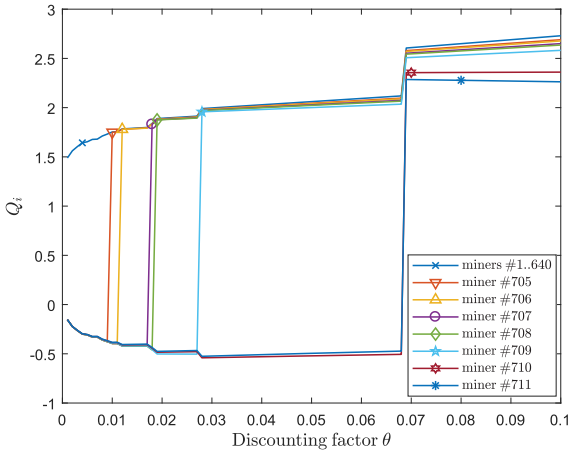

Figure 7: Indicator Q_i of relative change of cumulative utility for exponential discounting function, initial power of pool #1, $P_1^* = 0.3$.

From the results it is observable that, under exponential discounting function, indicator Q_i is decreasing with P_1^*. This is explained by the impact of a more powerful pool #2 on miners with $b_i(E_0) = 1$. In equilibrium, the lower estimate for its power is $1 - P_1^*$. This fosters faster compensation for smaller P_1^*.

Value of Q_i is increasing with θ. That is explained by the importance of time discounting which is increasing. This amplifies the incentives to join more powerful pool for miners with $b_i(E_0) = 1$.

Finally, the effect of equilibrium between the two pools is not equal for different miners. Under the same discount parameter θ, indicator Q_i is comparable for all except few most powerful miners, which performance is significantly worse.

This is due to the fact that they face a tough dilemma between benefiting from their (substantial) past contributions in pool #1 or faster future reward in pool #2.

IV. Discussion

Our model describes the incentives of miners to join different PPLNS pools. It takes into account the essential aspects of pooled mining, including compensation of past contributions as well as expected reward for her future activity. The latter is analysed using standard time discounting, which has strong implications for the model outcomes. Based on the proposed model we conclude that under the condition $N_1 = N_2$ miners will tend to migrate from smaller to larger PPLNS pools. It should be stressed that without time discounting $\mathcal{D}_{1,i} = \mathcal{D}_{2,i}$ (see eq. (3)), which means none of the miners has an incentive to leave their initial pool. Hence, game theoretical models that do not include time discounting may underestimate the existing risk of centralization in PoW cryptocurrencies.

It is important to consider the beliefs of the miners and substantiate how they align with the future observations. This us done by analyzing a special case where we proposed definition 1 and demonstrated in lemmas 1 and 2 that the proposed beliefs are indeed consistent. As a result, an equilibrium exists in the system of two pools and should be reached at moment E_0. The Result of corollary 1 supports our thesis that miners with lower mining power have stronger incentive to abandon smaller pool in favor of a larger one. This allowed to design an efficient method to find Nash equilibrium which complexity is only $O(n)$. The property discussed in corollary 1 is more profound for the case of higher time preference which is defined by parameter θ, and disproportionally divided mining power of the pools which is defined by value of P_1^*. For example, from fig. 5 it can be noticed that under very moderate intensity of time discounting, near half of the pool hash power is fleeing to a larger pool if the initial power distribution between two PPLNS pools is 30% vs 70%.

Our study of the changes in mining power of PPLNS pools with the same size of reward window can be interpreted for the systems with more than two pools. For such case, the incentives to leave a pool can be calculated by comparing individual utilities of independent miners in that pool with the utilities that can be obtained by the miners in the most powerful pool in the system.

The redistribution of mining power can cause a negative effect on decentralized governance of cryptocurrencies, their resilience to attacks, and public trust. As a practical recommendation to the administrators of PPLNS pools, the authors suggest to control incentives of the affiliated miners by adjusting the size of rewarding windows for each pool individually. The intuition to such recommendation can be gained from eq. (5) and the fact that $\theta = kE_N$. For instance, for k that is the same for both pools, condition $\frac{\Psi_{1,i}}{E_{N,1}} \geq \frac{\Psi_{2,i}}{E_{N,2}}$ is sufficient to make utility $\tilde{U}_i(E_0)$ positive. Yet another approach to avoid deterioration of the pool performance is to compose it only from miners whose individual power is higher than corresponding SIP (fig. 6).

Our results may seem contradictory to previous research on this topic. This is due to the specifics of PPLNS and time discounting, two essential factors often not taken into account in modelling exercises. For example, [5] concludes non-existence of equilibria. We, on the other hand, demonstrate that there is an equilibrium in the system of PPLNS pools. The argument that supports our statement can be found in the utility eq. (5) which contains components representing a fraction of past contribution of miner i in the pool of her initial membership. In the alternative pool, this component cannot be immediately obtained, which reflects the inertia of the system, thus making frequent migration between the pools hardly rational.

In future work, we plan to investigate scenarios of a higher complexity including: larger number of competing pools; different sizes of PPLNS reward window, and different time preferences for different miners.

V. Conclusions

In this paper, we analyzed miner-driven redistribution of mining power between the pools supporting PoW cryptocurrencies. We looked at competition between two PPLNS pools with the same parameter N. This is explained by the fact that PPLNS pools constitute significant part of mining power in PoW blockchains [4], [8]. This redistribution has a direct effect on centralization, which in turn leads to severe and harmful attacks [20], [21].

We proposed a new game theoretical model describing miners incentives to migrate between the pools and designed an efficient method to find Nash equilibrium. Our model highlights the importance of realistic and documented behavioural assumptions in models of decision making in the context of pooled mining. In particular, time preferences here are shown to play a crucial role in the predictions of the model and its security implications. To the best of authors expertise, this is the first case of utilizing inter-temporal utility in modelling of miners incentives to migrate between the pools.

Our results demonstrate that even moderate time discounting can cause migration of miners from smaller pools to larger pools. These results are obtained when modelling specific features of human behavior (i.e., time discounting) as well as specifics of pool mining (PPLNS). We thus posit that the effect of different mining schemes in centralisation is underplayed in discussions about security.

Finally, we provide an intuition for how the negative effects of power redistribution can be mitigated by individually adjusting the parameter N – window size – in each of the competing PPLNS pools.

References

[1] Nakamoto, Satoshi, "Bitcoin: A peer-to-peer electronic cash system", 2008, Online; accessed 29 January 2016.

[2] G. Malavolta, P. Moreno-Sanchez, A. Kate, M. Maffei, and S. Ravi, "Concurrency and privacy with payment-channel networks", in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '17, Dallas, Texas, USA: ACM, 2017, pp. 455–471, ISBN: 978-1-4503-4946-8. DOI: 10.1145/3133956.3134096. [Online]. Available: http://doi.acm.org/10.1145/3133956.3134096.

[3] I. Giechaskiel, C. Cremers, and K. B. Rasmussen, "When the crypto in cryptocurrencies breaks: Bitcoin security under broken primitives", *IEEE Security & Privacy*, 2018. [Online]. Available: https://publications.cispa.saarland/2656/.

[4] Y. Zolotavkin, J. García, and C. Rudolph, "Incentive compatibility of pay per last n shares in bitcoin mining pools", in *Decision and Game Theory for Security*, S. Rass, B. An, C. Kiekintveld, F. Fang, and S. Schauer, Eds., Cham: Springer International Publishing, 2017, pp. 21–39, ISBN: 978-3-319-68711-7.

[5] Y. Lewenberg, Y. Bachrach, Y. Sompolinsky, A. Zohar, and J. S. Rosenschein, "Bitcoin mining pools: A cooperative game theoretic analysis", in *Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems*, ser. AAMAS '15, Istanbul, Turkey: International Foundation for Autonomous Agents and Multiagent Systems, 2015, pp. 919–927, ISBN: 978-1-4503-3413-6. [Online]. Available: http://dl.acm.org/citation.cfm?id=2772879.2773270.

[6] A. Zamyatin, K. Wolter, S. Werner, P. G. Harrison, C. E. A. Mulligan, and W. J. Knottenbelt, "Swimming with fishes and sharks: Beneath the surface of queue-based ethereum mining pools", in *2017 IEEE 25th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*, Sep. 2017, pp. 99–109. DOI: 10.1109/MASCOTS.2017.22.

[7] R. Qin, Y. Yuan, S. Wang, and F. Wang, "Economic issues in bitcoin mining and blockchain research", in *2018 IEEE Intelligent Vehicles Symposium (IV)*, Jun. 2018, pp. 268–273. DOI: 10.1109/IVS.2018.8500377.

[8] M. Rosenfeld, "Analysis of bitcoin pooled mining reward systems", *arXiv preprint arXiv:1112.4980*, 2011.

[9] J. J. G. Chávez and C. K. da Silva Rodrigues, "Automatic hopping among pools and distributed applications in the bitcoin network", in *2016 XXI Symposium on Signal Processing, Images and Artificial Vision (STSIVA)*, Aug. 2016, pp. 1–7. DOI: 10.1109/STSIVA.2016.7743340.

[10] B. Fisch, R. Pass, and A. Shelat, "Socially optimal mining pools", in *Web and Internet Economics*, N. R. Devanur and P. Lu, Eds., Cham: Springer International Publishing, 2017, pp. 205–218, ISBN: 978-3-319-71924-5.

[11] E. Angner, *A Course in Behavioral Economics*. Palgrave Macmillan, 2012, ISBN: 9781137017512.

[12] S. Frederick, G. Loewenstein, and T. O'Donoghue, "Time discounting and time preference: A critical review", *Journal of Economic Literature*, vol. 40, no. 2, pp. 351–401, 2002, ISSN: 00220515. [Online]. Available: http://www.jstor.org/stable/2698382.

[13] Kano pool, "Pool payout", 2017, Online; accessed August 13, 2018.

[14] BCmonster, "Mining Statistics", 2018, Online; accessed September 22, 2018.

[15] Coinlend, *Automated margin lending: A possibility for passive income with cryptocurrencies*, Press Release, https://www.coinspeaker.com/automated-margin-lending-a-possibility-for-passive-income-with-cryptocurrencies/, 2018.

[16] D. Smith, *Reliability, Maintainability and Risk: Practical Methods for Engineers including Reliability Centred Maintenance and Safety-Related Systems*. Elsevier Science, 2011, ISBN: 9780080969039. [Online]. Available: https://www.elsevier.com/books/reliability-maintainability-and-risk/smith/978-0-08-096902-2.

[17] F. Arnold, H. Hermanns, R. Pulungan, and M. Stoelinga, "Time-dependent analysis of attacks", in *Principles of Security and Trust*, M. Abadi and S. Kremer, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 285–305, ISBN: 978-3-642-54792-8.

[18] G. O. Karame, E. Androulaki, and S. Capkun, "Double-spending fast payments in bitcoin", in *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, ser. CCS '12, Raleigh, North Carolina, USA: ACM, 2012, pp. 906–917, ISBN: 978-1-4503-1651-4. DOI: 10.1145/2382196.2382292. [Online]. Available: http://doi.acm.org/10.1145/2382196.2382292.

[19] J. A. Kroll, I. C. Davey, and E. W. Felten, "The economics of bitcoin mining, or bitcoin in the presence of adversaries", in *Proceedings of WEIS*, vol. 2013, 2013, p. 11. [Online]. Available: https://pdfs.semanticscholar.org/c55a/6c95b869938b817ed3fe3ea482bc65a7206b.pdf.

[20] G. O. Karame, E. Androulaki, M. Roeschlin, A. Gervais, and S. Čapkun, "Misbehavior in bitcoin: A study of double-spending and accountability", *ACM Trans. Inf. Syst. Secur.*, vol. 18, no. 1, 2:1–2:32, May 2015, ISSN: 1094-9224. DOI: 10.1145/2732196. [Online]. Available: http://doi.acm.org/10.1145/2732196.

[21] I. Eyal, "The miner's dilemma", in *2015 IEEE Symposium on Security and Privacy*, May 2015, pp. 89–103. DOI: 10.1109/SP.2015.13.

[22] K. Chatterjee, A. K. Goharshady, R. Ibsen-Jensen, and Y. Velner, "Ergodic Mean-Payoff Games for the Analysis of Attacks in Crypto-Currencies", in *29th International Conference on Concurrency Theory (CONCUR 2018)*, S. Schewe and L. Zhang, Eds., ser. Leibniz International Proceedings in Informatics (LIPIcs), vol. 118, Dagstuhl, Germany: Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2018, 11:1–

11:17, ISBN: 978-3-95977-087-3. DOI: 10.4230/LIPIcs.CONCUR.2018.11. [Online]. Available: http://drops.dagstuhl.de/opus/volltexte/2018/9549.

[23] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable", *Commun. ACM*, vol. 61, no. 7, pp. 95–102, Jun. 2018, ISSN: 0001-0782. DOI: 10.1145/3212998. [Online]. Available: http://doi.acm.org/10.1145/3212998.

[24] K. Nayak, S. Kumar, A. Miller, and E. Shi, "Stubborn mining: Generalizing selfish mining and combining with an eclipse attack", in *2016 IEEE European Symposium on Security and Privacy (EuroS P)*, Mar. 2016, pp. 305–320. DOI: 10.1109/EuroSP.2016.32.

[25] H. Liu, N. Ruan, R. Du, and W. Jia, "On the strategy and behavior of bitcoin mining with n-attackers", in *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, ser. ASIACCS '18, Incheon, Republic of Korea: ACM, 2018, pp. 357–368, ISBN: 978-1-4503-5576-6. DOI: 10.1145/3196494.3196512. [Online]. Available: http://doi.acm.org/10.1145/3196494.3196512.

[26] S. Bag, S. Ruj, and K. Sakurai, "Bitcoin block withholding attack: Analysis and mitigation", *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 8, pp. 1967–1978, Aug. 2017, ISSN: 1556-6013. DOI: 10.1109/TIFS.2016.2623588.

[27] S. Yoo, S. Kim, J. Joy, and M. Gerla, "Promoting cooperative strategies on proof-of-work blockchain", in *2018 International Joint Conference on Neural Networks (IJCNN)*, Jul. 2018, pp. 1–8. DOI: 10.1109/IJCNN.2018.8489267.

[28] O. Schrijvers, J. Bonneau, D. Boneh, and T. Roughgarden, "Incentive compatibility of bitcoin mining pool reward functions", in *Financial Cryptography and Data Security: 20th International Conference, FC 2016, Christ Church, Barbados, February 22–26, 2016, Revised Selected Papers*, J. Grossklags and B. Preneel, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2017, pp. 477–498, ISBN: 978-3-662-54970-4. DOI: 10.1007/978-3-662-54970-4_28. [Online]. Available: https://doi.org/10.1007/978-3-662-54970-4_28.

[29] Z. Li and Q. Liao, "Toward socially optimal bitcoin mining", in *2018 5th International Conference on Information Science and Control Engineering (ICISCE)*, Jul. 2018, pp. 582–586. DOI: 10.1109/ICISCE.2018.00126.

Appendix A
Remark

Remark 1. *[Larger pool discounts less] We consider* 2 *pools for which mining power is expressed with the functions* $\psi^{'}(E)$ *and* $\psi^{''}(E)$ *for pool #1 and pool #2, respectively.*

$$\forall E \geq E_0\Big(\psi^{''}(E) \geq \psi^{'}(E) \geq 0\Big)\wedge\left(\int_{E_0}^{E^{''}}\psi^{'}(E)\,\mathrm{d}E = \int_{E_0}^{E^{'}}\psi^{''}(E)\,\mathrm{d}E\right)\vdash$$
$$\vdash \int_{E_0}^{E^{'}} f(E-E_0)\psi^{''}(E)\,\mathrm{d}E \geq \int_{E_0}^{E^{''}} f(E-E_0)\psi^{'}(E)\,\mathrm{d}E$$

if the discounting function $f(E-E_0) \geq 0$ *is monotonically decreasing on* $E \in [E_0, \infty)$*. (See section A)*

Proof. Clearly, $E^{''} \geq E^{'}$ as otherwise $\int_{E_0}^{E^{''}}\psi^{'}(E)\,\mathrm{d}E < \int_{E_0}^{E^{'}}\psi^{''}(E)\,\mathrm{d}E$. We analyze $\int_{E_0}^{E^{'}} f(E-E_0)\psi^{''}(E)\,\mathrm{d}E - \int_{E_0}^{E^{''}} f(E-E_0)\psi^{'}(E)\,\mathrm{d}E = \int_{E_0}^{E^{'}} f(E-E_0)\Big(\psi^{''}(E)-\psi^{'}(E)\Big)\mathrm{d}E - \int_{E^{'}}^{E^{''}} f(E-E_0)\psi^{'}(E)\,\mathrm{d}E$. Because $f(E-E_0)$ is monotonically decreasing, $\int_{E_0}^{E^{'}} f(E-E_0)\Big(\psi^{''}(E)-\psi^{'}(E)\Big)\mathrm{d}E \geq f(E^{'}-E_0)\int_{E_0}^{E^{'}}\Big(\psi^{''}(E)-\psi^{'}(E)\Big)\mathrm{d}E$ and $\int_{E^{'}}^{E^{''}} f(E-E_0)\psi^{'}(E)\,\mathrm{d}E \leq f(E^{'}-E_0)\int_{E^{'}}^{E^{''}}\psi^{'}(E)\,\mathrm{d}E$. Finally, we point out that $f(E^{'}-E_0)\int_{E_0}^{E^{'}}\Big(\psi^{''}(E)-\psi^{'}(E)\Big)\mathrm{d}E - f(E^{'}-E_0)\int_{E^{'}}^{E^{''}}\psi^{'}(E)\,\mathrm{d}E = f(E^{'}-E_0)\left(\int_{E_0}^{E^{'}}\psi^{''}(E)\,\mathrm{d}E - \int_{E_0}^{E^{''}}\psi^{'}(E)\,\mathrm{d}E\right) = 0$ according to the premise of the argument. □

Appendix B
Lemmas

Lemma 1. $\forall E^{'}, E^{''}$ *if* $\Big(\forall j \in \mathbf{M}_2\Big(P_1^* + p_j < 0.5\Big) \wedge \Big(E^{''} \geq E^{'} \geq E_0\Big)\Big)$ *then* $\mathbf{M}_2^{E^{'}} \subseteq \mathbf{M}_2^{E^{''}}$.

Proof. For the validity, it is sufficient to substantiate the following two arguments:

(a) $\forall E^{'}\Big(\forall j \in \mathbf{M}_2\Big(P_1^* + p_j < 0.5\Big) \wedge \Big(E^{'} \geq E_0\Big) \vdash \Big(\mathbf{M}_2 \subseteq \mathbf{M}_2^{E^{'}}\Big)\Big)$,

(b) $\forall E^{'}, E^{''}\Big(\forall j \in \mathbf{M}_2\Big(P_1^* + p_j < 0.5\Big) \wedge \Big(E^{''} \geq E^{'} \geq E_0\Big) \vdash \Big(\mathbf{M}_2^{E^{'}} \setminus \mathbf{M}_2 \subseteq \mathbf{M}_2^{E^{''}} \setminus \mathbf{M}_2\Big)\Big)$,

where $\mathbf{M}_2^{E^{'}} \setminus \mathbf{M}_2 = \mathbf{M}_2^{E^{'}} \cap (\mathbf{M}_2)^{\mathsf{c}}$ and $\mathbf{M}_2^{E^{''}} \setminus \mathbf{M}_2 = \mathbf{M}_2^{E^{''}} \cap (\mathbf{M}_2)^{\mathsf{c}}$ represent relative complements of set $\mathbf{M}_2$ in the sets $\mathbf{M}_2^{E^{'}}$ and $\mathbf{M}_2^{E^{''}}$, respectively.

For item (a) we proceed as follows. According to proof by contradiction, let us assume that

$$\exists E^{'}\Big(\forall j \in \mathbf{M}_2\Big(P_1^* + p_j < 0.5\Big) \wedge \Big(E^{'} \geq E_0\Big) \wedge \Big(\mathbf{M}_2 \nsubseteq \mathbf{M}_2^{E^{'}}\Big)\Big).$$

This means that $\exists j\Big(j \in \mathbf{M}_2 \wedge j \notin \mathbf{M}_2^{E^{'}}\Big)$ which implies that there is a moment $E^* \in \Big[E_0, E^{'}\Big]$ when miner j decides to switch her mining activity from pool #2 to pool #1 and, hence, $b_j(E^*) = 0$. We regard the case when $\tilde{U}_j(E^*) = F_{j,1}(E^*) + \mathcal{D}_{1,j}(E^*) - F_{j,2}(E^*) - \mathcal{D}_{2,j}(E^*) > 0$.

At the moment E^* miner j does not have any contribution in pool #1 and $F_{j,1}(E^*) = 0$. It is therefore necessary that $\mathcal{D}_{1,j}(E^*) - \mathcal{D}_{2,j}(E^*) > 0$, which contradicts with the result of remark 1 . This signifies that miners from pool #2 never switch their mining to pool #1 if premise of item (a) is true.

Now, let us consider item (b). According to the principle of proof by contradiction, we suppose that

$$\exists E^{'}, E^{''}\Big(\forall j \in \mathbf{M}_2\Big(P_1^* + p_j < 0.5\Big) \wedge \Big(E^{''} \geq E^{'} \geq E_0\Big) \wedge \Big(\mathbf{M}_2^{E^{'}} \setminus \mathbf{M}_2 \nsubseteq \mathbf{M}_2^{E^{''}} \setminus \mathbf{M}_2\Big)\Big).$$

This requires that $\exists i\Big(i \in \mathbf{M}_2^{E^{'}} \setminus \mathbf{M}_2 \wedge i \notin \mathbf{M}_2^{E^{''}} \setminus \mathbf{M}_2\Big)$. In that regard, we distinguish two moments $E^* \in \Big[E_0, E^{'}\Big]$ and $E^{**} \in \Big[E^{'}\, E^{''}\Big]$ when miner i first moved from pool #1 to pool #2 and first moved from pool #2 to pool #1, respectively. Further we will analyze incentives of miner i assuming that she is the first miner that leaves pool #2:

$$\forall E^{'}, E^{''}\Big(\forall j \neq i\Big(E^{''} \geq E^{'} \geq E_0\Big)\wedge\Big(b_j(E^{'}) = 1\Big)\wedge\Big(b_j(E^{''}) = 0\Big) \vdash$$
$$\vdash \Big(E^{''} \geq E^{**}\Big)\Big).$$

From the definition 1 we infer that at any moment $E \in [E^*, E^{**}]$ miner i estimates $\psi_{2,i}(E)$ on $E \in [E^*, \infty]$ as a non-decreasing function because she does not observe any other miner leaving pool #2. Correspondingly, any estimation $\psi_{1,i}(E)$ that is produced during $[E^*, E^{**}]$ is non-increasing on $E \in [E^*, \infty]$.

However, from the best responses eq. (4) $b_i(E^*) = 1$ and $b_i(E^{**}) = 0$, we infer that $\tilde{U}_i(E^*) < 0$ and $\tilde{U}_i(E^{**}) \geq 0$. According to eq. (3) this implies that $F_{i,1}(E^*) + \mathcal{D}_{1,i}(E^*) - F_{i,2}(E^*) - \mathcal{D}_{2,i}(E^*) < F_{i,1}(E^{**}) + \mathcal{D}_{1,i}(E^{**}) - F_{i,2}(E^{**}) - \mathcal{D}_{2,i}(E^{**})$. We arrive to a contradiction: i) $F_{i,1}(E^*) - F_{i,1}(E^{**}) \geq 0$ because contribution of the miner in pool #1 cannot increase while she is in pool #2; ii) $F_{i,2}(E^*) - F_{i,2}(E^{**}) \leq 0$ because contribution in pool #2 increases as she is mining for that pool; iii) $\mathcal{D}_{1,i}(E^*) - \mathcal{D}_{1,i}(E^{**}) \geq 0$ because $\psi_{1,i}(E)$ is non-increasing; iv) $\mathcal{D}_{2,i}(E^*) - \mathcal{D}_{2,i}(E^{**}) \leq 0$ because $\psi_{2,i}(E)$ is non-decreasing.

We complete the proof by noting that validity of item (a) and item (b) implies that

$$\forall E^{'}, E^{''}\Big(\forall j \in \mathbf{M}_2\Big(P_1^* + p_j < 0.5\Big) \wedge \Big(E^{''} \geq E^{'} \geq E_0\Big) \vdash$$
$$\vdash \Big(\mathbf{M}_2^{E^{'}} \subseteq \mathbf{M}_2^{E^{''}}\Big)\Big)$$

is valid. □

Lemma 2. *$\forall E^{'}$ if $\Big(\forall j \in \mathbf{M}_2\big(P_1^* + p_j < 0.5\big) \wedge \big(E^{'} \geq E_0\big)\Big)$ then $\mathbf{M}_1^{E_0} \subseteq \mathbf{M}_1^{E^{'}}$.*

Proof. We question validity of the argument by analyzing the truth value of the contradicting statement:

$$\exists E^{'}\Big(\forall j \in \mathbf{M}_2\big(P_1^* + p_j < 0.5\big) \wedge \big(E^{'} > E_0\big) \wedge \big(\mathbf{M}_1^{E_0} \not\subseteq \mathbf{M}_1^{E^{'}}\big)\Big),$$

meaning that $\exists i\left(i \in \mathbf{M}_1^{E_0} \wedge i \notin \mathbf{M}_1^{E^{'}}\right)$. We analyze incentives of miner i who is the first miner that leaves pool #1 at the moment $E^* \in \left(E_0,\, E^{'}\right]$ providing that argument:

$$\forall E\Big(\forall j \neq i\big(E > E_0\big) \wedge \big(b_j(E_0) = 0\big) \wedge \big(b_j(E) = 1\big) \vdash \big(E \geq E^*\big)\Big)$$

is valid.

Let us consider best responses of i at E_0 and E^*. According to eq. (4), values $b_i(E_0) = 0$ and $b_i(E^*) = 1$ require that $\tilde{U}_i\left(E_0\right) \geq 0$ and $\tilde{U}_i\left(E^*\right) < 0$. From eq. (3), this implies that $F_{i,1}\left(E_0\right) + \mathcal{D}_{1,i}(E_0) - F_{i,2}\left(E_0\right) - \mathcal{D}_{2,i}(E_0) > F_{i,1}\left(E^*\right) + \mathcal{D}_{1,i}(E^*) - F_{i,2}\left(E^*\right) - \mathcal{D}_{2,i}(E^*)$. We arrive to a contradiction: i) $F_{i,1}\left(E_0\right) - F_{i,1}\left(E^*\right) \leq 0$ because fractional contribution of the miner in pool #1 is non-decreasing as she continues to mine there and no miner ever switches to pool #1 from pool #2 (according to lemma 1); ii) $F_{i,2}\left(E_0\right) - F_{i,2}\left(E^*\right) = 0$ because the miner does not contribute to pool #2 on $(E_0,\, E^*]$; iii) $\mathcal{D}_{1,i}(E_0) - \mathcal{D}_{1,i}(E^*) = 0$, and iv) $\mathcal{D}_{2,i}(E_0) - \mathcal{D}_{2,i}(E^*) = 0$ because according to the definition, no transition happens on $(E_0,\, E^*]$ in the direction from pool #1 to pool #2, and, no transition ever happens in the direction from pool #2 to pool #1 (according to lemma 1). □

Appendix C
Corollary

Corollary 1. *Under exponential discounting, $\forall \Psi_{1,i}$, $\forall \theta \leq 0.5\left(\partial \frac{\tilde{U}_i(E_0)}{\partial p_i} \geq 0\right)$.*

Proof. According to the definition 1, $\Psi_{2,i} = 1 - \Psi_{1,i} + p_i$, which we substitute into eq. (5), $\tilde{U}_i\left(E_0\right) = \frac{p_i}{P_1^*} + \frac{\Psi_{1,i}}{\theta}\left(1 - e^{-\frac{\theta}{\Psi_{1,i}}}\right) - \frac{1-\Psi_{1,i}+p_i}{\theta}\left(1 - e^{-\frac{\theta}{1-\Psi_{1,i}+p_i}}\right)$. For the sake of simplicity, we abandon index i and use $\tilde{U}$ instead of $\tilde{U}\left(E_0\right)$. Let us analyze conditions when $\partial \frac{\tilde{U}}{\partial p} \geq 0$:

$$\partial \frac{\tilde{U}}{\partial p} = \frac{1}{P_1^*} - \frac{1}{\theta} + \frac{1}{\theta} e^{-\frac{\theta}{1-\Psi_1+p}} + \frac{1}{1-\Psi_1+p} e^{-\frac{\theta}{1-\Psi_1+p}} \geq 0\,.$$

Using lemma 1 we conclude that $P_1^* \geq \Psi_1$. According to the initial assumption $P_1^* \leq 0.5$ and, therefore $\frac{1}{1-\Psi_1+p} \leq \frac{1}{P_1^*}$. This provides

$$\partial \frac{\tilde{U}}{\partial p} \geq \frac{1}{1-\Psi_1+p} - \frac{1}{\theta} + \frac{1}{\theta} e^{-\frac{\theta}{1-\Psi_1+p}} + \frac{1}{1-\Psi_1+p} e^{-\frac{\theta}{1-\Psi_1+p}}\,.$$

We question conditions that make the right part of the last inequality positive, which requires that $e^{-\frac{\theta}{1-\Psi_1+p}} \geq 1 - \frac{2\theta}{1-\Psi_1+p+\theta}$. On the other hand, it can be observed that inequality $e^{-\frac{2\theta}{1-\Psi_1+p+\theta}} \geq 1 - \frac{2\theta}{1-\Psi_1+p+\theta}$ is always satisfied. For our task it is sufficient to define conditions when $e^{-\frac{\theta}{1-\Psi_1+p}} \geq e^{-\frac{2\theta}{1-\Psi_1+p+\theta}}$. We arrive to $\frac{2\theta}{1-\Psi_1+p+\theta} \geq \frac{\theta}{1-\Psi_1+p}$, where sufficient condition is $\theta \in [0,\, 0.5]$. □

Appendix D
Cumulative utility of miners from pool #1

Cumulative utility of miners under equilibrium

Depending on miner's i best response $b_i(E_0)$ in equilibrium she either remains in pool #1 or moves to pool #2. We recall expressions for the corresponding utility functions at $E^{'} \geq E_0$:

$$U_{i,1}\left(E^{'}\right) = Rp_i \Pr\left(\mathbb{B}\,\middle|\,\Delta E\right)\left(F_{i,1}\left(E^{'}\right) + \mathcal{D}_{1,i}(E^{'})\right),$$

$$U_{i,2}\left(E^{'}\right) = Rp_i \Pr\left(\mathbb{B}\,\middle|\,\Delta E\right)\left(F_{i,2}\left(E^{'}\right) + \mathcal{D}_{2,i}(E^{'})\right).$$

For simplicity, we abandon multiplier $Rp_i \Pr\left(\mathbb{B}\,\middle|\,\Delta E\right)$ which is neither affected by the choice of miner i nor changes with time. In addition, in equilibrium every miner knows exact power of pool #1, Ψ_1, and pool #2, $1 - \Psi_1$, and, hence, we use $\mathcal{D}_1$, $\mathcal{D}_2$ instead of $\mathcal{D}_{1,i}$, $\mathcal{D}_{2,i}$, respectively. Cumulative utility function of miner $i \in \mathbf{M}_1$ is calculated over $E^{'} \in [E_0,\, \infty)$:

$$C_{i,1} = \int_{E_0}^{\infty} \left(F_{i,1}\left(E^{'}\right) + \mathcal{D}_1(E^{'})\right) \mathrm{d}E^{'}\,,$$

$$C_{i,2} = \int_{E_0}^{\infty} \left(F_{i,2}\left(E^{'}\right) + \mathcal{D}_2(E^{'})\right) \mathrm{d}E^{'}\,,$$

where the fractions of the past contribution of miner i into pool #1 and #2 are

$$F_{i,1}\left(E^{'}\right) = \begin{cases} \left(1 - \Psi_1 \frac{E^{'} - E_0}{E_N}\right) F_{i,1}\left(E_0\right) f\left(E^{'} - E_0\right), & \text{if } E^{'} \leq E_0 + \frac{E_N}{\Psi_1}; \\ 0, & \text{if } E^{'} > E_0 + \frac{E_N}{\Psi_1}, \end{cases}$$

$$F_{i,2}\left(E^{'}\right) = 0\,.$$

Discount factors $\mathcal{D}_1$ and $\mathcal{D}_2$ are computed as following:

$$\mathcal{D}_1\left(E^{'}\right) = \frac{1}{E_N} \int_{E^{'}}^{E^{'} + \frac{E_N}{\Psi_1}} \Psi_1 f\left(E - E_0\right) \mathrm{d}E\,,\ \mathcal{D}_2\left(E^{'}\right) = \frac{1}{E_N} \int_{E^{'}}^{E^{'} + \frac{E_N}{1-\Psi_1}} \left(1 - \Psi_1\right) f(E - E_0)\, \mathrm{d}E\,.$$

We express $C_{i,1}$ and $C_{i,2}$ taking into account that $F_{i,1}\left(E_0\right) = \frac{p_i}{P_1^*}$. For exponential discounting function, $f\left(E - E_0\right) = e^{-\theta \frac{E - E_0}{E_N}}$, therefore

$$C_{i,1} = \frac{p_i}{P_1^*} \int_{E_0}^{E_0 + \frac{E_N}{\Psi_1}} \left(1 - \Psi_1 \frac{E^{'} - E_0}{E_N}\right) e^{-\theta \frac{E^{'} - E_0}{E_N}} \mathrm{d}E^{'} + \frac{\Psi}{E_N} \int_{E_0}^{\infty} \mathrm{d}E^{'} \int_{E^{'}}^{E^{'} + \frac{E_N}{\Psi_1}} e^{-\theta \frac{E - E_0}{E_N}}\, \mathrm{d}E\,,$$

$$C_{i,2} = \frac{1 - \Psi}{E_N} \int_{E_0}^{\infty} \mathrm{d}E^{'} \int_{E^{'}}^{E^{'} + \frac{E_N}{1-\Psi_1}} e^{-\theta \frac{E - E_0}{E_N}}\, \mathrm{d}E\,.$$

Cumulative utility of miners for "no competition – no move" scenario

For the hypothetical scenario of "no move" $\forall i \in \mathbf{M}_1$, $b_i(E_0) = 0$. Thus, we only compute $C^*_{i,1}$ for a special case $\Psi_1 = P^*_1$. Cumulative utility for exponential time-discounting

$$C^*_{i,1} = \frac{p_i}{P^*_1} \int\limits_{E_0}^{E_0+\frac{E_N}{P^*_1}} \left(1 - P^*_1 \frac{E' - E_0}{E_N}\right) e^{-\theta \frac{E'-E_0}{E_N}} \mathrm{d}E' + \frac{P^*_1}{E_N} \int\limits_{E_0}^{\infty} \mathrm{d}E' \int\limits_{E'}^{E'+\frac{E_N}{P^*_1}} e^{-\theta \frac{E-E_0}{E_N}} \mathrm{d}E \,.$$