IFIP Networking 2019 1570511975

Incentives for Stable Mining in Pay Per Last *N* Shares Pools

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

***Abstract*—A large number of blockchain consensus protocols use the Proof of Work (PoW) principle, which relies on miners who exchange computation for newly minted currency. Their task is to support consensus, safeguarding the immutability of the chain's history. For the sake of regular income, a vast majority of miners team-up in large independent pools. These pools distribute among all their members the rewards gathered from individual miners, thus guaranteeing a stable income for each miner in the pool. The monetary compensation follows a specific reward system enforced by the pool administrator. Pay Per Last N Shares (PPLNS) is one of the most popular reward systems in PoW pools. Despite many desirable properties, in this paper, we show that composition of PPLNS pools may be unstable. To better understand the incentives of miners, we explore the effect of time preferences in the mining decisions of miners. Using a game-theoretical model we study conditions for equilibrium in a game with two different PPLNS pools. We find that the range of parameters that support equilibria between the pools with large number of miners is minuscule. This implies that in many cases, miners may have incentives to migrate towards larger pools, harming decentralization in the process.**

***Index Terms*—cryptocurrency, blockchain, proof of work, decentralization, game theory, time discounting**

I. Introduction

Proof-of-Work (PoW) is the principle behind decentralisation in the vast majority of modern cryptocurrencies. In PoW cryptocurrencies, consensus is reached by having miners solve computation puzzles [1]. Miners exchange their computational effort for the opportunity to earn a monetary payoff [2], [3]. Solo mining entails large income variances. Since miners prefer stable income, solo mining is very rare and instead, miners assemble themselves in pools. Inside pools the benefits from newly discovered blocks are shared by all pool members in proportion to their individual efforts. All miners solve puzzles of low complexity, known as "shares". On submission, every share is rewarded by the pool manager in proportion to its complexity. The pool, however, profits when the full solution of a block puzzle randomly appears among the shares. This scheme ensures a stable compensation for all the miners. Pools have different reward schemes, determining how the work done by miners in their shares translates into currency compensation [4], [5].

Many reward schemes (e.g., Pay Per Share – PPS, Proportional reward – PROP) are vulnerable to "pool hopping". This issue arises because rational miners can increase their returns by switching their mining activity between different pools [6]. The main advantage of PPLNS pools is its resilience to "pool hopping" [7]–[9]. PPLNS will only reward the N most recent shares preceding a discovered block, thereby encouraging pool loyalty. Figure 1 depicts the case for $N = 20$ shares. According to this schematic figure, the sliding window for the most recent payment contains 8 shares produced by miner A and 12 shares produced by miner B. Hence, these miners are eligible for 0.4 and 0.6 of the reward, respectively. The parameter N varies across different pools [10], [11]. The interaction between

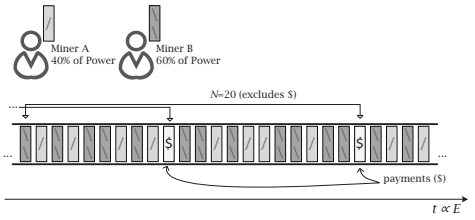


Figure 1. Rewards in PPLNS pool with two miners

behaviour and mining incentives has been previously studied using game theoretical models [12]–[15]. The idea of these models is to explore how different protocols and parameters play along with miners that are rational decision makers. The goal for most of the protocols in the light of strategic thinking is to provide incentives that are aligned with desirable properties of the system.

We present a game theoretical model to study the incentives of miners in PPLNS pools. Importantly, we allow for miners to discount time. This is a well-known feature of decision makers whose choices are rewarded in the future. It is particularly important for PPLNS given the time features introduced by the reward windows. Our models shows that agents may have incentives to migrate. This is done by studying the trade-off between leaving and staying in your current pool, when pools have different aggregate computational power and different sizes of reward window N.

Models of time discounting study valuation discrepancies that rational agents have about rewards that they receive at different points in time. For example, by comparing person's valuation at an earlier date with one for a later date illustrates that present valuations are higher than future ones [16]. There are multiple reasons that can explain the differences in valuations, e.g., the opportunity to invest earlier rewards and earn

ISBN 978-3-903176-16-4

interests on them [17], [18]. In addition, for the infrastructure run by a pool manager which accounts mining contributions of the miners, risks of hardware failure or risks associated with compromised cybersecurity add up with the time [19], [20]. This also should discount expected future compensation. In order to express miner incentives, our model uses time preferences with exponential discounting, as commonly used model in economics.

It remains unclear why the option of faster compensation in PPLNS pools has attracted so little attention from the community [8]. 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, rewards for the previous efforts will be received by the miners at a slower pace. On the other hand, for stable mining it is sufficient if none of the miners leaves her pool. Our model demonstrates that, for example, disproportion in the power of two PPLNS pools with the same size of reward window N may motivate miners to relocate to the larger pool. Another form of imbalance may occur between the pools of comparable power but different sizes of reward windows. This process accelerates in the pools that either have higher number of miners or have higher time-preference.

The lack of incentives for steady mining may cause depletion and disappearance of smaller PPLNS pools which will create pool market that is dominated by a handful of very large pools. Such centralization of power, runs counter to the intent of cryptocurrencies and produces an environment which is opportune to a number of harmful attacks [12], [14], [21]. Based on our model, we suggest how the disparity between PPLNS pools can be analyzed and mitigated.

The rest of this paper is organized as follows. A game-theoretical model for stable mining in two PPLNS pools is presented in section II. Individual contributions of miners to their pool are expressed as the amount of energy that was spent on mining. Given approach simplifies modeling and analysis of the properties of the system of two PPLNS pools. Conditions that support stable mining in the system of two PPLNS pools are analyzed in section III. It includes experimental simulations that assist us in extending the domains for the parameters that sustain equilibrium. Results are discussed and concluded in section IV.

II. A game-theoretical model for stable mining

We define stable mining as an equilibrium in the system of two PPLNS pools where none of the miners has an incentive to leave her original pool. Specifying the miners' incentives requires detailed analysis of the process of mining and defining the utility of each miner. In order to accomplish this task we start with a single PPLNS pool where we represent mining as a continuous process.

A. Discrete and continuous models of PPLNS mining in a single pool

Mining in PPLNS pool requires the submission of shares at discrete moments in time, however, the assumption that the computational complexity of a single share is small, allows us to represent mining with a continuous model. The mining energy E (consumed by all miners) is a central parameter of the model and can be seen as equivalent to the time t that measures the duration of mining process.

We assume that all the shares produced by the miners and submitted to the pool are of equal computational complexity. The computational efficiency of the mining equipment of all the miners is equal and remains stable throughout the mining duration. Hence, we conclude that the production of every share requires equal amount of electrical energy. This property is used to measure total computational effort (of any given miner and on any time interval) in terms of energy spent in computation. Throughout the paper, we ignore network delays and assume that individual mining effort is immediately recorded by the mining pool.

Our model for miner incentives considers the effect from producing an elementary mining effort at time t_0, with duration $\Delta t \to 0$. As an example, we will refer to miners A and B, who contribute 40% and 60% of total power, respectively – see fig. 2. The power of the pool (pool #1) is denoted P_1. The total power of the system is then $P = P_1 = P_A + P_B = 1$ – in general, if there is more than one pool in the system, $P \geq P_1$. Thus, we consider the computation of a share requires energy $\Delta E = P_1 \Delta t = \Delta t$.

We will draw an analogy between discrete and continuous models and express the corresponding utilities of miner A (fig. 2). Different components of the utility will be analyzed. In order to illustrate this analogy, we will separately discuss: a) past contributions of a miner in the most recent PPLNS window of size N and her incentive to reward this contribution by her current mining effort delivered to this pool; b) time-discounting for the future compensation of her current mining effort.

1) Utility of miner A arising from the past: For miner A, we express the mining effort that has been contributed prior to moment t_0 (past, denoted as $\mathcal{P}$ on fig. 2), and an expected compensation of this contribution as a result of her mining at t_0.

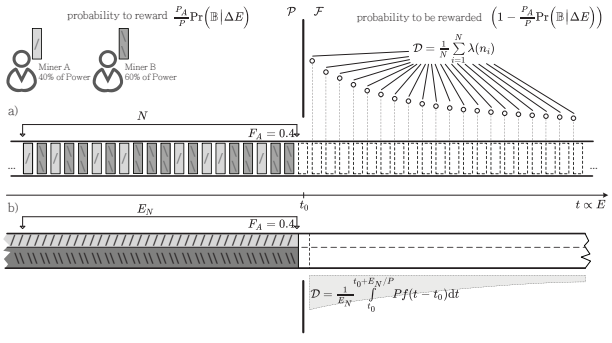


Figure 2. Analogy between discrete and continuous models for mining in PPLNS pool

In the discrete model, for any share that arrived in the pool, the probability that it was produced by miner A is $\frac{P_A}{P_1}$. We calculate the proportion of her shares in the most recent window of size N: $F_A = \frac{N_A}{N}$, where $N_A = \sum_{i=1}^{N} \frac{P_A}{P_1}$ is the number of shares (in expectation) that were produced by miner A. This implies that $F_A = \frac{P_A}{P_1}$.

In the continuous model, the contribution of miner A is measured as a fraction $F_A = \frac{E_{A,N}}{E_N}$. Here, E_N is the energy necessary to produce N shares, $E_N = N\Delta E$, and, $E_{A,N}$ is the energy consumed by miner A during time $\frac{E_N}{P_1}$, which is computed as $E_{A,N} = \int_0^{E_N} \frac{P_A}{P_1} \mathrm{d}E = \int_0^{N\Delta E} \frac{P_A}{P_1} \mathrm{d}E = \frac{P_A}{P_1} N\Delta E$. As a result, $F_A = \frac{P_A}{P_1}$ in the continuous model as well.

If miner A continues to work for the pool at t_0, she self-compensates her past contribution F_A. The effect of instant self-compensation for miner A is the expectation of immediate reward, obtained as a result of her mining during $[t_0, t_0 + \Delta t]$. In the discrete model, the elementary contribution is represented by a share that is produced in the pool and on average requires effort ΔE (fig. 2). With probability $\frac{P_A}{P_1}$ this share is delivered by miner A. This elementary contribution has a chance to become a full solution (to produce a new block $\mathbb{B}$ on the blockchain). The probability to deliver a full solution as a result of spending ΔE will be denoted $\Pr\big(\mathbb{B} \,\big|\, \Delta E\big)$. In this case, the reward R will be distributed between miners A and B, where miner A will receive her fraction, F_A. As a result, miner A expects to receive an instant self-compensation equal to $F_A \frac{P_A}{P_1} R \cdot \Pr\big(\mathbb{B} \,\big|\, \Delta E\big)$.

In the continuous case, we also consider a portion ΔE, produced by the pool at t_0 (see fig. 2). Effort ΔE_A is the direct contribution of miner A. It may result in finding a full solution, which will provide miner A with compensation $F_A R$. Considering the properties of PoW mining, we infer that $\Pr\big(\mathbb{B} \,\big|\, \Delta E_A\big) = \Pr\big(\mathbb{B} \,\big|\, \frac{P_A}{P_1}\Delta E\big) = \frac{P_A}{P_1}\Pr\big(\mathbb{B} \,\big|\, \Delta E\big)$. Therefore, in such model, the expected utility for miner A, associated with her past performance is also $F_A \frac{P_A}{P_1} R \cdot \Pr\big(\mathbb{B} \,\big|\, \Delta E\big)$.

2) Utility of miner A arising in the future: For miner A, we express the future compensation and corresponding discounting of the current mining effort that is produced during $[t_0, t_0 + \Delta t]$ – the process of compensation in the future is denoted with $\mathcal{F}$ on fig. 2. With probability $\Big(1 - \frac{P_A}{P_1}\Pr\big(\mathbb{B} \,\big|\, \Delta E\big)\Big)$ her elementary effort does not result in finding $\mathbb{B}$, she expects to receive a corresponding reward in a gradual manner, later, as long as her elementary contribution is part of the most recent reward window.

Time discounting is a common approach to valuate reward that is ought to be received in the future [16]. It reflects the preference that rational agents have toward monetary compensation received instantly compared to the equal compensation to be obtained in the future [16].

In the discrete case, the share will be rewarded as long as it remains inside current window of size N. We assume N to be large enough and $\Pr\big(\mathbb{B} \;\big|\; \Delta E\big)$ is small. Hence, every subsequent share in the pool in expectation rewards the elementary contribution of miner A with $\frac{P_A}{P_1}\frac{R}{N}\Pr\big(\mathbb{B} \,\big|\, \Delta E\big)$.

The rate at which shares arrive to the pool is constant and depends on the power P_1. For instance, i shares that arrive into the pool since moment $t_0 + \Delta t$ require $n_i = \frac{iP}{P_1}$ elementary time intervals Δt. The corresponding time-discounting coefficient for the compensation induced by share i is denoted as $\forall i \lambda(n_i) \in (0, 1)$, $\forall i \in \mathbb{N}\big(\lambda(n_i) > \lambda(n_{i+1})\big)$. Therefore, the total valuation for miner A's future reward is $\Big(1 - \frac{P_A}{P_1}\Pr\big(\mathbb{B} \,\big|\, \Delta E\big)\Big) \frac{P_A}{P_1} R \Pr\big(\mathbb{B} \;\big|\; \Delta E\big) \frac{1}{N} \sum_{i=1}^{N} \lambda(n_i)$. The parameter $\mathcal{D} = \frac{1}{N} \sum_{i=1}^{N} \lambda(n_i)$ is the complete discounting coefficient.

In the continuous model, the portion of energy $\frac{P_A}{P_1}\Delta E$ is delivered by miner A during $[t_0, t_0 + \Delta t]$. It is therefore rewarded at every moment $t > t_0 + \Delta t$, with $R\frac{P_A}{P_1}\frac{\Delta E}{E_N}\Pr\big(\mathbb{B} \;\big|\; \Delta E\big) = R\frac{P_A}{P_1}\frac{P_1 \Delta t}{E_N}\Pr\big(\mathbb{B} \;\big|\; \Delta E\big)$ in expectation. To the reward awarded in the future, miner A applies continuous decreasing time-discounting function $f(t - t_0)$, such that $(\forall t \geq t_0)\big(f(t - t_0) \in (0, 1)\big)$. The rewarding process lasts $\frac{E_N}{P_1}$ and covers time interval $\left[t_0, t_0 + \frac{E_N}{P_1}\right]$. Hence, for miner A, the future component of the reward is $\Big(1 - \frac{P_A}{P_1}\Pr\big(\mathbb{B} \,\big|\, \Delta E\big)\Big) \frac{P_A}{P_1} R \Pr\big(\mathbb{B} \,\big|\, \Delta E\big) \frac{1}{E_N} \int_{t_0}^{t_0 + E_N/P_1} P_1 f(t - t_0) \mathrm{d}t$. The parameter $\mathcal{D} = \frac{1}{E_N} \int_{t_0}^{t_0 + E_N/P_1} P_1 f(t - t_0) \mathrm{d}t$ can be used to designate complete time-discounting coefficient for the effort of miner A in continuous model.

Now, let us compare expressions for $\mathcal{D}$ for discrete and continuous cases. We consider exponential discounting, commonly used in game theory and behavioral economics [17]. For the discrete model we will use $\lambda(n_i) = \delta^{n_i}$, $\delta \in (0, 1)$, while for the continuous model we will use $f(t - t_0) = e^{-k(t - t_0)}$. For the continuous case, we have

$$\mathcal{D} = \frac{1}{E_N} \int_{t_0}^{t_0 + E_N/P_1} P_1 e^{-k(t - t_0)} \mathrm{d}t = \frac{1}{N} \sum_{i=1}^{N} e^{-ik\frac{\Delta E}{P_1}},$$

which we now will compare with the discrete case

$$\mathcal{D} = \frac{1}{N} \sum_{i=1}^{N} \delta^{n_i}.$$

For the discrete case, it is assumed that $n_i = iC$, where $C \in \mathbb{R}^+$ is a constant expressing the intensity of time discounting for future compensation in the pool. We use property $e = \lim_{\Delta E \to 0} \big(1 - \Delta E\big)^{-\frac{1}{\Delta E}}$ to demonstrate that discrete and continuous discounting are equivalent if

$$\delta = 1 - \Delta E\,,\; C = \frac{k}{P_1}\,.$$

3) Total utility of miner A in discrete and continuous models: The total utility expresses the effect of incremental mining activity of miner A at moment t_0 on her monetary valuations. It takes into account past and future performance of the pool. The corresponding complete utility of miner A in discrete and continuous models is

$$U_A = \frac{P_A}{P_1} R \Pr\big(\mathbb{B} \,\big|\, \Delta E\big) \left[F_A + \left(1 - \frac{P_A}{P_1}\Pr\big(\mathbb{B} \,\big|\, \Delta E\big)\right)\mathcal{D}\right].$$

Because $\lim_{\Delta E \to 0} \Pr\big(\mathbb{B} \,\big|\, \Delta E\big) = 0$ we can further refer to a simplified expression of the utility:

$$U_A = \frac{P_A}{P_1} R\Pr\Big(\mathbb{B}\,\Big|\,\Delta E\Big)\Big[F_A + \mathcal{D}\Big].$$

For the provided example of mining in a pool, discrete and continuous models differ only in their expression for the time-discounting coefficient $\mathcal{D}$. For the sake of mathematical tractability, we will work with the continuous model in the remaining of the paper.

We will further ask what incentives are required for miners to uninterruptedly remain in their original pool, even in the presence of other PPLNS pools with different power and reward windows. We will focus on an extended version of this mining system, including two PPLNS pools.

B. Incentives with two PPLNS pools

Here we consider two PPLNS pools that have different power and window sizes. Miners in each of the pools are free to switch pools. We investigate the conditions required for miners to avoid switching, remaining in their original pools.

For each miner who is a member of a particular pool we compare the utility they would derive from mining in pool #1 versus pool #2. Without loss of generality, we assume the total power in the system is 1 and the power of pool #1 is $P_1 \le 0.5$. The reward windows are N_1 and N_2 shares long, and parameters $E_{N,1}$ and $E_{N,2}$ represent the energy each pool requires to mine N_1 and N_2 shares respectively. We use disjoint sets $\mathbf{M}_1$ and $\mathbf{M}_2$ to denote pool membership. For example, $i \in \mathbf{M}_1$ indicates that miner i belongs to pool #1.

For each miner i, we compare the utility values $U_{i,1}$ and $U_{i,2}$, gathered from mining in pool #1 and pool #2, respectively. For that miner, corresponding fractional contributions that are delivered in the past to each of the pools will be denoted $F_{i,1}$ and $F_{i,2}$, respectively. The discount coefficient for the future reward in pool #1 is $\mathcal{D}_{1,i}$, discounting for future reward in pool #2 is $\mathcal{D}_{2,i}$.

For any miner i from pool #1, whose individual power is p_i, her past contribution in the most recent PPLNS window (capacity $E_{N,1}$) of that pool is $F_{i,1} = \frac{p_i}{P_1}$. In pool #2, her past contribution is $F_{i,2} = 0$. For any miner j from pool #2, her past contribution in pool #1 is $F_{j,1} = 0$, and contribution to pool #2 is $F_{j,2} = \frac{p_j}{1-P_1}$.

Let us discuss the values of coefficients $\mathcal{D}_{1,i}$ and $\mathcal{D}_{2,i}$ for miner $i \in \mathbf{M}_1$. Since we analyze a special case when miners are incentivized to mine uninterruptedly in their pools, incentives of miner i are calculated under assumption that all the other miners do not change their pool memberships. If the miner stays in pool #1, the total power of the pool is equal to P_1 and her elementary contribution of mining energy $p_i\Delta t = p_i\Delta E$ at moment t_0 will be compensated during timeframe $\left[t_0,\, t_0 + \frac{E_{N,1}}{P_1}\right]$. If the miner moves to pool #2, the total power of that pool will be equal to $1 - P_1 + p_i$ and the elementary contribution of mining energy $p_i\Delta E$ of that miner will be compensated during period $\left[t_0,\, t_0 + \frac{E_{N,2}}{1-P_1+p_i}\right]$. Therefore, for each of the decisions of miner i we compute discount coefficients as follows:

$$\mathcal{D}_{1,i} = \frac{1}{E_{N,1}} \int_{t_0}^{t_0+E_{N,1}/P_1} P_1 f(t-t_0)\mathrm{d}t\,,$$

$$\mathcal{D}_{2,i} = \frac{1}{E_{N,2}} \int_{t_0}^{t_0+E_{N,2}/(1-P_1+p_i)} (1-P_1+p_i)\, f(t-t_0)\mathrm{d}t\,.$$

In a similar manner, for miner $j \in \mathbf{M}_2$ the discounting coefficients related to the move to pool #1 and to steady mining in pool #2 are

$$\mathcal{D}_{1,j} = \frac{1}{E_{N,1}} \int_{t_0}^{t_0+E_{N,1}/\left(P_1+p_j\right)} \left(P_1+p_j\right) f(t-t_0)\mathrm{d}t\,,$$

$$\mathcal{D}_{2,j} = \frac{1}{E_{N,2}} \int_{t_0}^{t_0+E_{N,2}/(1-P_1)} (1-P_1)\, f(t-t_0)\mathrm{d}t\,,$$

respectively.

In order to decide whether to mine steadily in her pool or to migrate to the other, every miner needs to compare these utilities. For example, miner $i \in \mathbf{M}_1$ will continue to mine in pool #1 if and only if $U_{i,1} - U_{i,2} = p_i R\Pr\Big(\mathbb{B}\,\Big|\,\Delta E\Big)\Big[F_{i,1} + \mathcal{D}_{1,i} - F_{i,2} - \mathcal{D}_{2,i}\Big]$ is non-negative. Likewise, miner $j \in \mathbf{M}_2$ will remain loyal to pool #2 if and only if $U_{j,1} - U_{j,2} = p_j R\Pr\Big(\mathbb{B}\,\Big|\,\Delta E\Big)\Big[F_{j,1} + \mathcal{D}_{1,j} - F_{j,2} - \mathcal{D}_{2,j}\Big] \le 0$. Since $p_i R\Pr\Big(\mathbb{B}\,\Big|\,\Delta E\Big)$, $p_j R\Pr\Big(\mathbb{B}\,\Big|\,\Delta E\Big)$ are non-negative, we can simplify to obtain utilities U_i and U_j:

$$\begin{cases} U_i = F_{i,1} + \mathcal{D}_{1,i} - F_{i,2} - \mathcal{D}_{2,i}\,, \\ U_j = F_{j,1} + \mathcal{D}_{1,j} - F_{j,2} - \mathcal{D}_{2,j}\,, \end{cases} \tag{1}$$

such that $\mathrm{sgn}\Big(U_i\Big) = \mathrm{sgn}\Big(U_{i,1} - U_{i,2}\Big)$ and $\mathrm{sgn}\Big(U_j\Big) = \mathrm{sgn}\Big(U_{j,1} - U_{j,2}\Big)$. For all players to stay put in their pools, we therefore require:

$$\forall i, j\Big(\Big((i \in \mathbf{M}_1) \vdash (U_i \ge 0)\Big) \wedge \Big((j \in \mathbf{M}_2) \vdash (U_j \le 0)\Big)\Big). \tag{2}$$

We next discuss in detail what is required for this "stable mining" condition to hold.

III. Requirements for stable mining

In order to determine equilibrium conditions, we assume, without loss of generality that $E_{N,1} \ne E_{N,2}$. Since the total power of the system is 1 we use time t and energy E interchangeably. Following eqs. (1) and (2), equilibrium between the pools requires that:

$$\begin{cases} U_i(E_0) = \dfrac{p_i}{P_1} + \dfrac{1}{E_{N,1}} \displaystyle\int_{E_0}^{E_0+\frac{E_{N,1}}{P_1}} f(E-E_0)\, P_1 \mathrm{d}E \\ \qquad\qquad - \dfrac{1}{E_{N,2}} \displaystyle\int_{E_0}^{E_0+\frac{E_{N,2}}{1-P_1+p_i}} f(E-E_0)\,(1-P_1+p_i)\mathrm{d}E \qquad \ge 0\,, \\ U_j(E_0) = -\dfrac{p_j}{1-P_1} - \dfrac{1}{E_{N,2}} \displaystyle\int_{E_0}^{E_0+\frac{E_{N,2}}{1-P_1}} f(E-E_0)\,(1-P_1)\mathrm{d}E \\ \qquad\qquad + \dfrac{1}{E_{N,1}} \displaystyle\int_{E_0}^{E_0+\frac{E_{N,1}}{P_1+p_j}} f(E-E_0)\left(P_1+p_j\right)\mathrm{d}E \qquad \le 0\,. \end{cases}$$

As is customary [16], we use an exponential function for discounting:

$$f(E-E_0) = e^{-\theta\frac{(E-E_0)}{E_{N,1}}}, \tag{3}$$

where θ specifies intensity of time-discounting. For example, if $\theta = 0.1$, miners at moment t_0 discount their compensation expected at time $t_0 + \frac{E_{N,1}}{P}$ with coefficient $e^{-0.1} \approx 0.9$. We will further express the quantities of interest in terms of the ratio $l = \frac{E_{N,2}}{E_{N,1}}$. Thus, using $E_{N,2} = lE_{N,1}$, we obtain:

$$\begin{cases} U_i(E_0) = \frac{p_i}{P_1} + \frac{P_1}{\theta}\left(1 - e^{-\frac{\theta}{P_1}}\right) \\ \qquad -\frac{1-P_1+p_i}{l\theta}\left(1 - e^{-\frac{l\theta}{1-P_1+p_i}}\right) \qquad \geq 0, \\ U_j(E_0) = -\frac{p_j}{1-P_1} - \frac{1-P_1}{l\theta}\left(1 - e^{-\frac{l\theta}{1-P_1}}\right) \\ \qquad +\frac{P_1+p_j}{\theta}\left(1 - e^{-\frac{\theta}{P_1+p_j}}\right) \qquad \leq 0. \end{cases} \tag{4}$$

To solve this system we first focus on low intensity of time-discounting (small θ), in which case we can find analytically a range of ratios l that satisfy the condition for given $\mathbf{M}_1$, $\mathbf{M}_2$. This will be discussed next. Later, Section III-B will deal with the case of arbitrary θ.

A. The case of small θ

For the first inequality in eq. (4) we use $e^{-\frac{l\theta}{1-P_1+p_i}} \geq 1 - \frac{l\theta}{1-P_1+p_i}$ to find the sufficient condition:

$$e^{\frac{\theta}{P_1}} \geq \frac{P_1^2}{P_1^2 - P_1\theta + p_i\theta}$$

where we require the denominator $P_1^2 - P_1\theta + p_i\theta \geq 0$ implying $\theta \leq \frac{P_1^2}{P_1 - p_i}$. We use the fact that $e^{\frac{\theta}{P_1}} \geq 1 + \frac{\theta}{P_1}$ and test the following sufficient condition:

$$1 + \frac{\theta}{P_1} \geq \frac{P_1^2}{P_1^2 - P_1\theta + p_i\theta},$$

which demands $\theta \leq \frac{p_i P_1}{P_1 - p_i}$. If the latter is satisfied, it implies that the assumption about the denominator is valid because $\forall i \in \mathbf{M}_1\ (P_1 \geq p_i)$.

For the second inequality in eq. (4) we use that $e^{-\frac{\theta}{P_1+p_j}} \geq 1 - \frac{\theta}{P_1+p_i}$ and state that

$$e^{\frac{l\theta}{1-P_1}} \geq \frac{(1-P_1)^2}{(1-P_1)^2 + p_j l\theta - l\theta(1-P_1)}$$

is sufficient if the denominator is positive, which requires $l\theta \leq \frac{(1-P_1)^2}{1-P_1-p_j}$. We use the fact $e^{\frac{l\theta}{1-P_1}} \geq 1 + \frac{l\theta}{1-P_1}$ and check the following condition

$$1 + \frac{l\theta}{1-P_1} \geq \frac{(1-P_1)^2}{(1-P_1)^2 + p_j l\theta - l\theta(1-P_1)},$$

which requires $l\theta \leq \frac{p_j(1-P_1)}{1-P_1-p_j}$. Satisfying the latter guarantees that the requirement for a positive denominator is also satisfied because $\forall j \in \mathbf{M}_2\left(1 - P_1 \geq p_j\right)$. Hence, for the system eq. (4) it is sufficient that

$$\begin{cases} \theta \leq \frac{p_i P_1}{P_1 - p_i}, \\ l\theta \leq \frac{p_j(1-P_1)}{1-P_1-p_j}. \end{cases} \tag{5}$$

The practical importance of this result may be particularly salient in small pools with relatively uniform distribution of mining power. In that situation, the first condition of 5 may be satisfied, leaving us with the less restrictive requirement of the second condition. In contrast to θ which represents preferences of the miners, parameter l here can be adjusted by the pool managers.

However, in larger pools that may include miners with small power, condition 5 is restrictive. Therefore, we next try to relax that constraint and deal with arbitrary values of θ.

B. The composition of stable mining pools

In this section we try to find pool compositions that, together with parameter l, are sufficient to guarantee pool stability for arbitrary values of θ. For this, let us analyze properties of miner utilities in each pool.

Remark 1: $\partial\frac{U_i}{\partial l} \geq 0$. To see this, note that $\partial\frac{U_i}{\partial l} = \frac{1-P_1+p_i}{l^2\theta}\left(1 - e^{-\frac{l\theta}{1-P_1+p_i}}\right) - \frac{1}{l}e^{-\frac{l\theta}{1-P_1+p_i}}$. For this quantity to be positive we require $e^{\frac{l\theta}{1-P_1+p_i}} \geq 1 + \frac{l\theta}{1-P_1+p_i}$, which is always true.
This remark shows that U_i is non-decreasing in l. This implies that $\forall i \in \mathbf{M}_1\left(l \geq \frac{1-P_1+p_i}{P_1}\right)$ is sufficient to discourage miners in pool #1 to migrate to pool #2 because at $l \geq \frac{1-P_1+p_i}{P_1}$ utility $U_i \geq \frac{p_i}{P_1}$. Another important consequence is that for every unique tuple $\left\{P_1,\ \theta,\ p_i\right\}$, $U_i = 0$ has at most one root in l.

In a similar manner, we will now show how l affects the utilities of miners in pool #2.

Remark 2: $\partial\frac{U_j}{\partial l} \geq 0$. To see this, note that $\partial\frac{U_j}{\partial l} = \frac{1-P_1}{l^2\theta}\left(1 - e^{-\frac{l\theta}{1-P_1}}\right) - \frac{1}{l}e^{-\frac{l\theta}{1-P_1}}$. For this quantity to be positive we require $e^{\frac{l\theta}{1-P_1}} \geq 1 + \frac{l\theta}{1-P_1}$, which is always true.
Hence, miners in pool #2 are discouraged to migrate to pool #1 if $\forall j \in \mathbf{M}_2\left(l \leq \frac{1-P_1}{P_1+p_j}\right)$.

Note that the utilities not only depend on l, but also on the power of the miners. Thus, we need to further investigate how this will affect stability.

Remark 3: $\forall l, \theta\left(\partial\frac{U_i}{\partial p_i} \geq 0\right)$. To see this, note that $\partial\frac{U_i}{\partial p_i} = \frac{1}{P_1} - \frac{1}{l\theta}\left(1 - e^{-\frac{l\theta}{1-P_1+p_i}}\right) + \frac{1}{1-P_1+p_i}e^{-\frac{l\theta}{1-P_1+p_i}}$. For this quantity to be positive we require $e^{-\frac{l\theta}{1-P_1+p_i}} \geq \frac{(P_1-l\theta)(1-P_1+p_i)}{P_1(1-P_1+p_i+l\theta)}$. This inequality is satisfied if $P_1 - l\theta \leq 0$. In case $P_1 - l\theta > 0$, we use that $e^{-\frac{l\theta}{1-P_1+p_i}} \geq 1 - \frac{l\theta}{1-P_1+p_i}$, it is sufficient that $1 - \frac{l\theta}{1-P_1+p_i} \geq \frac{(P_1-l\theta)(1-P_1+p_i)}{P_1(1-P_1+p_i+l\theta)}$. We arrive to $\frac{P_1(1-P_1+p_i)^2 - l\theta(1-P_1+p_i)^2}{P_1(1-P_1+p_i)^2 - P_1 l^2\theta^2} \leq 1$ which requires $(1-P_1+p_i)^2 \geq P_1 l\theta$. This is satisfied because $P_1 \leq 0.5$ and $P_1 - l\theta > 0$.

For the second pool, we cannot say much about $\partial\frac{U_j}{\partial p_j}$, since it requires further conditions on θ, and l. Instead, we consider the case when the first inequality in eq. (4) is satisfied and analyze the effect on the second inequality in eq. (4).

We discuss the dependency between l and p_i for a special case $U_i = 0$. A function $\mathcal{L}_0^1(p_i)$ will be used to define the corresponding ratio l. Using remark 1 and remark 3 we infer that $\mathcal{L}_0^1(p_i)$ should be non-increasing in p_i. The following result suggests that the second inequality in eq. (4) is satisfied for all pairs $\left\{p_j,\ \mathcal{L}_0^1(p_j)\right\}$.

Remark 4: $\forall l, \theta, p_i, p_j \Big((p_i = p_j) \vdash (U_i \geq U_j) \Big)$. We consider the case $p_i = p_j$, thus, for simplicity, individual indices will be omitted. Our statement requires the following:

$$\frac{p}{P_1} + \frac{P_1}{\theta}\left(1 - e^{-\frac{\theta}{P_1}}\right) - \frac{1-P_1+p}{l\theta}\left(1 - e^{-\frac{l\theta}{1-P_1+p}}\right) \geq$$
$$\geq -\frac{p}{1-P_1} - \frac{1-P_1}{l\theta}\left(1 - e^{-\frac{l\theta}{1-P_1}}\right) + \frac{P_1+p}{\theta}\left(1 - e^{-\frac{\theta}{P_1+p}}\right).$$

We use two facts: *i)* $-\frac{1-P_1+p}{l\theta}\left(1 - e^{-\frac{l\theta}{1-P_1+p}}\right) \geq -\frac{1-P_1+p}{l\theta}\left(1 - e^{-\frac{l\theta}{1-P_1}}\right)$ and *ii)* $\frac{P_1+p}{\theta}\left(1 - e^{-\frac{\theta}{P_1+p}}\right) \leq \frac{P_1+p}{\theta}\left(1 - e^{-\frac{\theta}{P_1}}\right)$, in order to check if the following (sufficient) condition holds.

$$\frac{p}{P_1} + \frac{P_1}{\theta}\left(1 - e^{-\frac{\theta}{P_1}}\right) - \frac{1-P_1+p}{l\theta}\left(1 - e^{-\frac{l\theta}{1-P_1}}\right) \geq$$
$$\geq -\frac{p}{1-P_1} - \frac{1-P_1}{l\theta}\left(1 - e^{-\frac{l\theta}{1-P_1}}\right) + \frac{P_1+p}{\theta}\left(1 - e^{-\frac{\theta}{P_1}}\right).$$

The latter can be presented as

$$p\left(\frac{1}{P_1} + \frac{1}{1-P_1}\right) \geq p\left(\frac{1}{\theta}\left(1 - e^{-\frac{\theta}{P_1}}\right) + \frac{1}{l\theta}\left(1 - e^{-\frac{l\theta}{1-P_1}}\right)\right),$$

which is satisfied because $\frac{\theta}{P_1} \geq 1 - e^{-\frac{\theta}{P_1}}$ and $\frac{l\theta}{1-P_1} \geq 1 - e^{-\frac{l\theta}{1-P_1}}$.

For $k \in \mathbf{M}$, $\mathbf{M} = \mathbf{M}_1 \cup \mathbf{M}_2$ we propose to define $\mathbf{M}_1$, $\mathbf{M}_2$ and l according to the following rule:

$$\begin{cases} \exists \ell^* \forall k \Big((p_k \geq p_{\ell^*} \vdash k \in \mathbf{M}_1) \wedge (p_k < p_{\ell^*} \vdash k \in \mathbf{M}_2) \Big); \\ \sum\limits_{\mathbf{M}_1} p_k = P_1; \\ l = \mathcal{L}_0^1(p_{\ell^*}). \end{cases} \tag{6}$$

Our task is to show that for any given allocation, $l = \mathcal{L}_0^1(p_{\ell^*})$ satisfies the inequalities in eq. (4).

We consider pool #1 and the first inequality in eq. (4). According to remarks 1 and 3 $\forall i \Big(i \geq \ell^* \vdash \mathcal{L}_0^1(p_{\ell^*}) \geq \mathcal{L}_0^1(p_i) \Big)$. Because U_i is non-decreasing on l, we conclude that $U_i \geq 0$ for $l = \mathcal{L}_0^1(p_{\ell^*})$.

Let us now consider pool #2 and the second inequality in eq. (4). We conclude that $U_j \leq 0$ because: a) from remark 4, the second inequality in eq. (4) is satisfied for all pairs $\Big\{ p_j, \mathcal{L}_0^1(p_j) \Big\}$; b) according to remarks 1 and 3 $\forall j \Big(j < \ell^* \vdash \mathcal{L}_0^1(p_{\ell^*}) \leq \mathcal{L}_0^1(p_j) \Big)$, and, according to remark 2 the value of U_j can not be higher for lower l.

We ask whether stable mining is possible: a) for values of l that differ from the requirement in eq. (6); b) for different allocations of miners in each pool. To answer this questions we use simulations, as discussed next.

C. Experimental evaluation

1) Description of the experiments: For different θ, P_1, we empirically reconstruct the functions $\mathcal{L}_0^1(p)$ and $\mathcal{L}_0^2(p)$. This will be used to analyze the allocation of miners into $\mathbf{M}_1$, $\mathbf{M}_2$, and the corresponding stability interval $[l_{\min}, l_{\max}]$ for l.

For stability we require:

$$\forall i, j \Big(\Big(i \in \mathbf{M}_1 \Big) \wedge \Big(j \in \mathbf{M}_2 \Big) \vdash$$
$$\vdash \Big(l_{\min} \leq l_{\max} \Big) \wedge \Big(\mathcal{L}_0^1(p_i) \leq l_{\min} \Big) \wedge \Big(\mathcal{L}_0^2(p_j) \geq l_{\max} \Big) \Big).$$

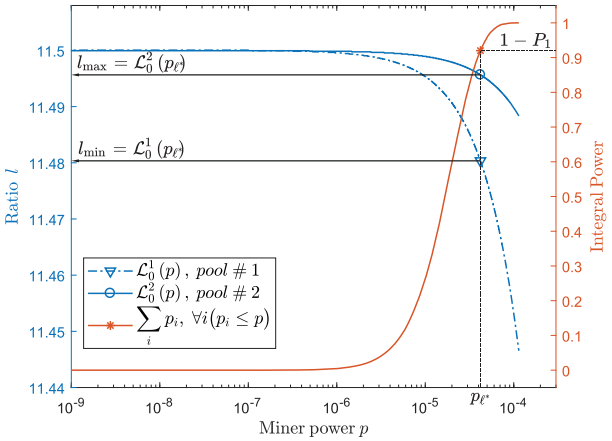
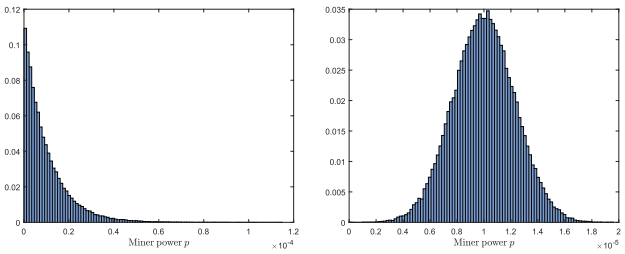


Figure 3. Defining $[l_{\min}, l_{\max}]$ using $\mathcal{L}_0^1(p)$ and $\mathcal{L}_0^2(p)$ for $P_1 = 0.08$, $\theta = 0.15$. Distribution of individual mining power in the system is exponential, $\lambda = 10^{-5}$, size of the set is 10^5.

To illustrate our methodology, let us discuss a particular example, depicted in fig. 3. Consider values $\theta = 0.15$ and $P_1 = 0.08$. Replacing these values in the expression for each of the utilities, U_i and U_j, (see eq. (4)), for each p, we solve l for $U_i = 0$, $U_j = 0$, respectively (for every $\{P_1, \theta, p\}$ tuple, there is at most one root on $l \in \mathbb{R}^+$, see remarks 1 and 2). We denote these roots $\mathcal{L}_0^1(p)$ and $\mathcal{L}_0^2(p)$. The power composition for both pools is drawn from the distribution shown in fig. 4a. In the interval of interest $p \in \left[10^{-9}, 10^{-4}\right]$, we can allocate miners to the pools and come up with a range of ratios l that guarantees that the system is in equilibrium.

We first note that: *i)* for every miner with power p in the pool #1, the ratio l that is higher than $\mathcal{L}_0^1(p)$ guarantees incentives to stay in the pool; *ii)* for every miner with power p in pool #2, the ratio l that is lower than $\mathcal{L}_0^2(p)$ also guarantees incentives to stay. Next, we will investigate the range $[l_{\min}, l_{\max}]$ for the allocation proposed in eq. (6). We find such threshold value p_{ℓ^*} to allocate miners to the pools: all the miners with power $p \geq p_{\ell^*}$ form pool #1, all the miners with power $p < p_{\ell^*}$ form pool #2. Finally, we define $l_{\min} = \mathcal{L}_0^1\Big(p_{\ell^*}\Big)$ and $l_{\max} = \mathcal{L}_0^2\Big(p_{\ell^*}\Big)$ as the endpoints for the interval of stability for l (see fig. 3). We will consider the size of this interval as a proxy for stability. Larger intervals imply, that under a certain distribution of power, we have a more stable system.



(a) Set of 10^5 samples, exponential pdf $\lambda e^{-\lambda p}$, $\lambda = 10^{-5}$.

(b) Set of 10^5 samples, normal pdf $m \approx 10^{-5}$, $\sigma \approx 2.3 \times 10^{-6}$.

Figure 4. Histograms of distribution of mining power p in the experimental sets.

In addition we also ask whether other allocations that provide larger $l_{\max} - l_{\min}$ are possible. In the experiment, both

$\mathcal{L}_0^1(p)$ and $\mathcal{L}_0^2(p)$ are monotonically decreasing, which implies that $l_{\min} = \mathcal{L}_0^1\big(\min_{i\in\mathbf{M}_1} p_i\big)$ and $l_{\max} = \mathcal{L}_0^2\big(\max_{j\in\mathbf{M}_2} p_j\big)$ for any chosen allocation $\mathbf{M}_1$, $\mathbf{M}_2$. These sets are exclusive, power of $\mathbf{M}_1$ members should sum up to P_1, and, hence, any allocation that is different to eq. (6) will either increase $l_{\min}$ or reduce $l_{\max}$.

Our further task is to analyze $[l_{\min}, l_{\max}]$ for different θ values. To represent different possible compositions of mining pools [10], [11], we use four sets of different size and power distribution in the experiments. We consider two main sizes, namely, set size 10^4 as equivalent to a pair of large pools; and set size 10^5, which may resemble, for instance, the whole BitCoin network divided in two pools. All the sets are normalized so that the total sum of values equals 1 (see figs. 4a and 4b).

2) Experimental results: The specific experimental conditions are as follows:

- Set size 10^4 samples, exponential pdf $\lambda_1 e^{-\lambda_1 x_1}$, $\lambda_1 = 10^{-4}$;
- Set size 10^4 samples, normal pdf, mean $m_1 \approx 10^{-4}$, standard deviation $\sigma_1 \approx 2.44 \times 10^{-5}$;
- Set size 10^5, exponential pdf $\lambda_2 e^{-\lambda_2 x_2}$, $\lambda_2 = 10^{-5}$;
- Set size 10^5, normal pdf, mean $m_2 \approx 10^{-5}$, standard deviation $\sigma_2 \approx 2.3 \times 10^{-6}$.

We choose in all cases an exponential distribution, explained by the fact that in practice, mining power is unevenly distributed among miners in the pool. Typically pool compositions are characterized by a majority of small-power miners together with a few very powerful participants (see for example the distribution in the Kano pool, [10]). Using this experimental setup, we ask, given a specific distribution of power, and using the allocation described in eq. (6), what is the resulting range of l that guarantees stability. The results of the experiment are depicted on figs. 5 and 6.

It can be seen that $l_{\max} - l_{\min}$ is smaller for the larger set containing 10^5 samples. This can be explained by the role of past contributions of the miners in their original pools. For larger pools, the power of a miner is small in relation to the pool power. Hence, such miner may have a higher incentive to leave her pool for a faster compensation in the other pool. This requires a tighter interval $[l_{\min}, l_{\max}]$ to support equilibrium, which makes stability in a system of PPLNS pools hardly achievable in practice. For all types of distribution and set sizes the size of $l_{\max} - l_{\min}$ decreases with θ. This is explained by the fact that prospects of faster compensation (in the other pool) become more important when compared to past contributions that remain unchanged.

The plots in figs. 5 and 6, show that all the points are located under the line $l = \frac{1-P_1}{P_1}$. This means that the windows sizes represented by l result in a situation without an equilibrium. However, it should be noted that many of the mining pools (especially those mining ETH, XMR, ZEC) define PPLNS pay-off window in units of time [22]. In these reward systems, it is common for many pools to have the same window sizes, which we will denote as T_N. For the case of two pools with power P_1 and $1 - P_1$ the energy capacity of the pay-off window is $T_N P_1$ and $T_N(1 - P_1)$, respectively. This results in $l = \frac{E_{N,2}}{E_{N,1}} = \frac{1-P_1}{P_1}$. According to our results, this value of l is the upper bound for $l_{\max}$ on the range of practical θ, and, therefore can not provide an equilibrium.

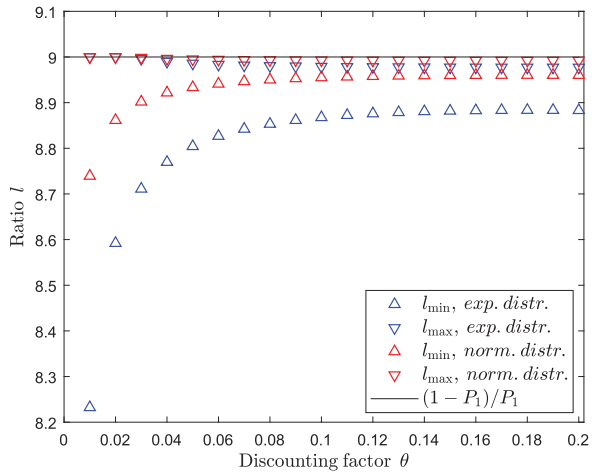


Figure 5. Endpoints $\{l_{\min}, l_{\max}\}$ under different θ and $P_1 = 0.1$. Calculated for exponential and normal distribution of samples, size of the set is 10^4.

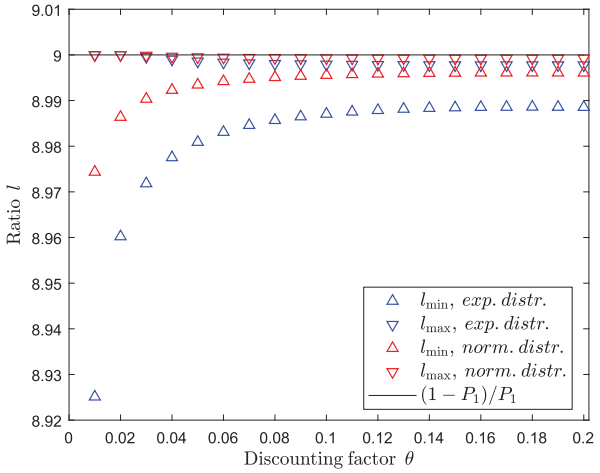


Figure 6. Endpoints $\{l_{\min}, l_{\max}\}$ under different θ and $P_1 = 0.1$. Calculated for exponential and normal distribution of samples, size of the set is 10^5.

Let us further consider examples where conditions for stable mining are not achievable. For the sake of comparing pools, we can express the amount of computed hashes as the equivalent of energy E that is spent on mining. As an example, we look at two Monero (XMR) PPLNS mining pools whose mining fees are equal and set to 1%. The mining power of the Monero Ocean pool [23] is equal to 7.8MH/sec, while the Nano pool has power 110MH/sec [22]. The pools interpret PPLNS reward windows differently. For Monero Ocean, the parameter N is measured in multiples of average XMR complexity, D, e.g. $N = 2D$. Given that (at the moment of paper preparation) average block complexity in XMR network is $D \approx 4.8 \times 10^{10}$ hashes, we infer that $E_{N,1} = 9.6 \times 10^{10}$. On the other hand, the Nano pool measures payout window in time units and sets it to 6 hours. Using its power estimate we infer that $E_{N,2} = 2.37 \times 10^{12}$. According to our results, the equilibrium value of $l = \frac{E_{N,2}}{E_{N,1}}$ should be slightly below $\frac{110\times10^6}{7.8\times10^6} \approx 14.1$, but, in practice this ratio is 24.69. This higher ratio l may

incentivize miners to leave the larger pool (Nano) and to join the smaller pool (Monero Ocean). This pattern of migration from large to small pools can potentially harm decentralization in the XMR network. Let us now consider a

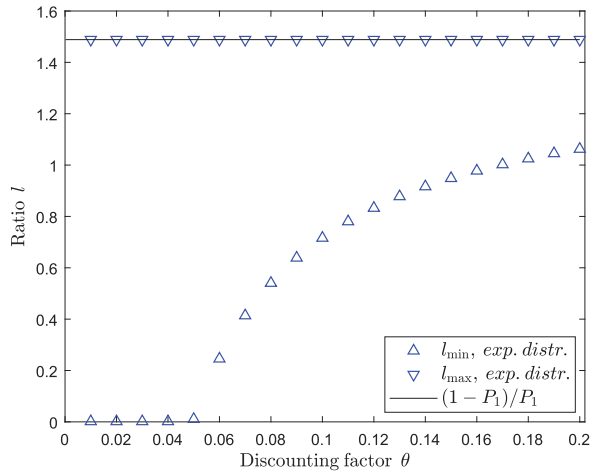


Figure 7. Interval of stability $[l_{\min}, l_{\max}]$ for the pair of PPLNS pools Monero Hash Vault and Monero Ocean based on the synthetic exponential distribution of individual power of miners, $\lambda = 10^{-2}$, size of the set is 10^2.

different pair of pools. For both XMR mining pools Monero Hash Vault [24] and Monero Ocean parameter, the PPLNS reward window is equal to $N = 2D$ meaning $E_{N,1} = E_{N,2}$. The mining power of Monero Hash Vault is only 5.24MH/sec implying that the equilibrium value for l should not be higher $l_{\max} < (1 - P_1)/P_1 \approx 1.49$. In practice this ratio l is set to 1. In order to decide if mining (in the system of these two pools) is stable we conducted an experiment. Since the mining power of both pools is relatively small, we use the set of 100 samples with exponential distribution of individual power in a simulation (see fig. 7). As it can be observed, the upper bound $l_{\max}$ is barely distinguishable from the constant 1.49 for the whole range of θ. In contrast, $l_{\min}$ increases rapidly in θ. The value of l stays in the range $[l_{\min}, l_{\max}]$ for $\theta \leq 0.17$. However, for more intense time discounting θ stable mining is not possible. Note than a larger number of miners – in the example 100 – will further constrain the conditions for stable mining. This situation may incentivize miners from the smaller pool to leave it for the prospect of higher utility in the larger pool.

This flow from small to larger pools can threathen certain pools, while also going against the spirit of the blockchain and its decentralization. It is common practice for pool administrators to set $N = k \times D$ where k is a small integer number, explaining why many pools have the same size (for instance, $k = 2$ or $k = 5$ is a popular choice) of reward window while their mining power may differ substantially. This common practice may exacerbate this problem.

IV. Discussion

We propose a game-theoretical model to study incentives for stable mining in the system of 2 PPLNS pools. We define the utility of individual miners as a function of energy E that they spend on mining in a particular pool. The model allows us to analyze the effect of time discounting on the rewards that will be received by the miners in the future. In order to express time preferences, we used standard exponential discounting (eq. (3)). We defined the conditions necessary for stable mining in a system with two pools, as a situation where no miner has incentives to leave her pool for the prospect of higher utility in a different pool (eq. (4)).

Stable mining requires that valuations of the past contributions plus future rewards in the original pool outweigh the expectation for future rewards in a different pool. In PPLNS pools with constant mining power this can be achieved by adjusting the sizes $E_{N,1}$, $E_{N,2}$ of the corresponding reward windows.

The condition we derive for stable mining may be applied in a system with more than 2 pools. In this case, it is sufficient that the condition for stable mining is satisfied for every pair of the pools.

Other parameters can also influence the incentives for miners to avoid switching pools, as outlined by the sufficient conditions for stable mining (see eqs. (5) and (6)). We also extend our results using simulations, which allows us to define a range $[l_{\min}, l_{\max}]$ of stable values for the ratio $l = \frac{E_{N,2}}{E_{N,1}}$, when we vary discounting θ and different distributions of individual mining power inside pools.

The range of acceptable values $[l_{\min}, l_{\max}]$ indicates how constrained is the equilibrium between the pools by the settings including size of the pools and discounting factor θ. From figs. 5 and 6 we can conclude that even for moderate time discounting θ the range of stability is rather small for the pools with substantially large number of miners.

Multiple outcomes are possible when the condition for stable mining in the system of two PPLNS pools is not satisfied. First, miners may have incentives to mine for each of the pools at different moments in time. It is difficult to assess what this implies for decentralization in PoW cryptocurrencies. Second, re-distribution may lead to other equilibria with favorable or unfavorable outcomes for decentralization. In this context, managers, who define values for $E_{N,1}$ and $E_{N,2}$ play an important role in the process of decentralization of PoW cryptocurrencies. Unfortunately, many PPLNS pools of different size have the same N which creates incentives for the miners from smaller pools to migrate toward the larger pools. This should be a subject of further research.

The proposed model for mining in PPLNS pools and the recommendations for the equilibrium ratio l can guide the choices of pool managers. In order to avoid negative effects associated with depleting pools, their reward windows need to be set accordingly.

One salient feature that we have not studied in this paper, is the strategic interactions between pool managers and their own incentives in setting window sizes. In the future, we also plan to extend this model to systems of many pools and different mining fees in the presence of network delays.

Our model is instrumental in highlighting the importance of accounting for realistic features of strategic behavior, e.g., time discounting, when analysing protocols for consensus.

References

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

[2] S. Dziembowski, "Introduction to cryptocurrencies", in *Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '15, Denver, Colorado, USA: ACM, 2015, pp. 1700–1701.

[3] 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.

[4] 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.

[5] 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)*, 2017, pp. 99–109.

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

[7] 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)*, 2016, pp. 1–7.

[8] 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.

[9] R. Qin, Y. Yuan, S. Wang, and F. Wang, "Economic issues in bitcoin mining and blockchain research", in *2018 IEEE Intelligent Vehicles Symposium (IV)*, 2018, pp. 268–273.

[10] Kano pool, *Pool payout*, https://kano.is/index.php?k=payout, Online; accessed August 13, 2018, 2018.

[11] BCmonster, *Mining Statistics*, http://www.bcmonster.com/index.php?page=statistics&action=pool, Online; accessed September 22, 2018, 2018.

[12] 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)*, vol. 118, Dagstuhl, Germany: Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2018, 11:1–11:17.

[13] 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*, Cham: Springer International Publishing, 2017, pp. 21–39.

[14] 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.

[15] Y. Kwon, D. Kim, Y. Son, E. Vasserman, and Y. Kim, "Be selfish and avoid dilemmas: Fork after withholding (faw) attacks on bitcoin", in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, ACM, 2017, pp. 195–209.

[16] 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.

[17] E. Angner, *A Course in Behavioral Economics*. Palgrave Macmillan, 2012.

[18] BlockFi, *Earn a 6.2% Annual Yield on Your Crypto*, https://blockfi.com/crypto-interest-account/, Online; accessed March 13, 2019, 2019.

[19] D. Smith, *Reliability, Maintainability and Risk: Practical Methods for Engineers including Reliability Centred Maintenance and Safety-Related Systems*. Elsevier Science, 2011.

[20] 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.

[21] I. Eyal, "The miner's dilemma", in *2015 IEEE Symposium on Security and Privacy*, 2015, pp. 89–103.

[22] Nano pool, *Pool hashrate*, https://xmr.nanopool.org/, Online; accessed November 13, 2018, 2018.

[23] Moneroocean, *Dashboard*, https://moneroocean.stream/#/dashboard, Online; accessed October 5, 2018, 2018.

[24] Monero Hash Vault, *Dashboard*, https://monero.hashvault.pro/en/dashboard, Online; accessed October 12, 2018, 2018.