Mining pool network and decentralization of a PoW blockchains

Hansjoerg Albrecher[1], Pierre-O. Goffard[2], and Bilel Tounsi[3]

[1]UNIL
[2]Université de Strasbourg
[3]UNIL

November 28, 2025

Abstract

The Proof-of-Work (PoW) blockchain relies on miners who incur constant operational costs while receiving stochastic rewards. To mitigate financial uncertainty, many miners join Pay-per-Share (PPS) mining pools, which provide stable payouts while transferring risk to pool managers. This paper analyzes miners' strategic choices using an expected discounted dividend approach. The pool managers surplus is modelled by a two-sided jump processes for which we show that barrier strategies are optimal under specific conditions. Numerical methods to determine optimal barriers and dividends are provided. Finally, we explore miner distributions across pools and investigate Nash equilibria, providing insights into competitive dynamics. Our findings contribute to understanding how economic incentives influence miner participation and the decentralization of PoW blockchain networks.

1 Introduction

The Proof-of-Work (PoW) blockchain consensus mechanism, as first introduced by **?**, forms the foundation of decentralized cryptocurrencies such as Bitcoin. This system relies on miners who expend computational resources to validate transactions and secure the network. However, mining is characterized by a dual-risk structure: miners face a constant operational cost (electricity, hardware maintenance) while their rewards—block subsidies and transaction fees—are inherently stochastic and infrequent. This financial uncertainty poses a significant challenge, as it directly impacts the sustainability of individual miners.

To mitigate this volatility, miners often choose to join mining pools. These pools aggregate computational power, distribute rewards more predictably, and ensure more stable revenue streams. Among the various pooling strategies, the Pay-per-Share (PPS) model [**???**] provides miners with a fixed payout per valid share they contribute, effectively transferring risk to the pool manager.

Miners must make a strategic decision regarding participation in a mining pool, balancing expected revenue against the risk of ruin. This decision can be analyzed using an expected discounted dividend approach, which evaluates the long-term viability of miners given their financial constraints. In this context, optimal dividend strategies, such as the barrier strategy [**?**], emerge as critical tools for sustaining miner operations and maximizing profitability. These strategies rely on results from fluctuation theory and scale functions [**?**] to determine optimal capital retention and payout policies.

While extensive research exists on individual miner strategies, the surplus process of the pool manager remains relatively unexplored. It can be modeled as a two-sided jump process, incorporating incoming miner contributions and outgoing payouts. However, existing literature provides limited results on optimal surplus management in this setting. In this paper, we establish that a band strategy is optimal in general and that a simple barrier strategy becomes under certain restrictions. We further develop numerical methods to identify the optimal barrier level and compute corresponding dividends.

Beyond individual miner and pool manager strategies, we leverage our findings to analyze the equilibrium distribution of miners across available mining pools. By considering a set of miners and a set of pool managers, we derive insights into how miners allocate their computational power in response to different payout schemes and risk profiles. Our study further extends to a numerical investigation of Nash equilibria, illustrating the strategic interactions between miners and pool managers in a competitive setting.

This research contributes to the ongoing discourse on decentralization in PoW blockchains. By providing a framework for mining pool strategies and decision-making, we offer insights into how economic incentives shape miner participation, thereby influencing the overall decentralization and stability of blockchain networks.

2 Wealth processes and dividends for miner and pool managers

A miner is characterized by her hashpower λ and her operational cost c. A PPS deal is characterized by a difficulty reeduction δ and a pool fee f.

2.1 Miners' wealth process

- Solo mining, the wealth of a miner is given by

  $$X_t = x - c \cdot t + N_t \cdot b, \text{ for } t \geq 0, \tag{1}$$

  where c is the operational cost of the miner, $(N_t)_{t\geq 0}$ is a Poisson process with intensity λ and b is the block reward.

- Mining in one pool with characteristics (δ, f), the wealth of the pool miner is given by

  $$\tilde{X}_t = x - c \cdot t + \tilde{N}_t \cdot \tilde{b}, \text{ for } t \geq 0, \tag{2}$$

  where $(N_t)_{t\geq 0}$ is a Poisson process with intensity $\tilde{\lambda} = \lambda/\delta$ and $\tilde{b} = (1-f)\cdot b \cdot \delta$ is the share reward.

- Mining in several pool: The wealth of a miner that splits her hashpower between several PPS mining pool with characteristics $(\delta_k, f_k)_{k=1,\dots,n}$ according to a weight vector

  $$w = \begin{pmatrix} w_0 & w_1 & \dots & w_n \end{pmatrix} \in \Delta^n,$$

  where $\Delta^n = \left\{ w \in \mathbb{R}^{n+1}; \sum_{i=0}^n w_i = 1 \right\}$ represents the unit simplex, is given by

  $$X_t = x - c \cdot t + \sum_{i=1}^{N_t} B_i, \tag{3}$$

  where

  - $(N_t)_{t\geq 0}$ is a Poisson process with intensity $\mu = \sum_{k=0}^n \mu_k$ and$\mu_k = \frac{\lambda w_k}{\delta_k}$, for $k = 0, \dots, n$.
  - the B_i values form a sequence of independent and identically distributed random variables with the following distribution

    $$\mathbb{P}(B = (1-f_k)\cdot b \cdot \delta_k) = \frac{\mu_k}{\mu} = p_k, \text{ for } k = 0, \dots, n.$$

2.2 Pool managers' wealth process

A PPS pool manager attracts miners by offering them PPS deals characterized by $(\delta_k, f_k)_{k=1,\dots,n}$. Miners then decide to invest or not in these PPS deals. The results isthat the pools collects a hashpower λ splitted according to a weight vector

$$w = \begin{pmatrix} w_1 & w_2 & \dots & w_n \end{pmatrix} \in \Delta^{n-1}.$$

The rate of arrival of each type of share is

$$\mu_k = \frac{w_k \lambda}{\delta_k}, k = 1, \dots, n,$$

A share from PPS deal k has probability $\delta_k/(1+\delta_k)$ of being an actual solution. The wealth of the pool manager is given by

$$Y_t = y + \sum_{i=1}^{M_t} V_i, \tag{4}$$

where

- $(M_t)_{t\geq 0}$ is a Poisson process with intensity $\mu = \sum_{k=1}^{n} \mu_k$
- The V_i's are iid with probability distribution

$$\mathbb{P}(V = -b \cdot (1-f_k) \cdot \delta_k) = \frac{\mu_k}{\mu} \frac{1}{1+\delta_k}, \text{ and } \mathbb{P}(V = b - b \cdot (1-f_k) \cdot \delta_k) = \frac{\mu_k}{\mu} \frac{\delta_k}{1+\delta_k}, \text{ for } k = 1, \dots, n.$$

Assumption 1. *We assume that each mining pool is only offering one type of PPS deal (δ, f) to the miners.*

Assumption 1 affects the distribution of the V_i's which simplifies to

$$\mathbb{P}(V = -w) = \frac{1}{1+\delta}, \text{ and } \mathbb{P}(V = b - w) = \frac{\delta}{1+\delta},$$

where $w = b \cdot (1-f) \cdot \delta$ denotes the reward for finding a share.

The drift condition is expressed as

$$\text{drift} = p(b-w) - qw > 0, \tag{5}$$

with $p = \frac{\delta}{1+\delta}$, $q = 1-p$, and $w = b(1-f)\delta$. Substituting these expressions into (6) leads to the inequality

$$\delta > \frac{w}{b-w}. \tag{6}$$

In practice, the jump intensity $\mu(f)$ emerges from miners' aggregate actions, with each miner's choice to enter or exit a pool driven by the contract pair (f, δ) set by the manager. The next section presents a criterion, based on a mean–variance trade-off, to determine a miner's entry decision.

3 Nash equilibrium through Mean-variance trade-offs optimization

3.1 Miner's mean–variance allocation among multiple mining venues

We consider a miner i who may distribute fractions of her computational power among several mutually exclusive mining modes. Let

$$w_i = (w_{i,0}, w_{i,1}, \dots, w_{i,n}), \qquad w_{i,k} \geq 0, \qquad \sum_{k=0}^{n} w_{i,k} = 1,$$

denote the vector of hashing weights allocated to solo mining ($k = 0$) and to each available pool ($k \geq 1$). Allocation is continuous: the miner may simultaneously participate in several pools by splitting her hashrate across venues.

Each mode k is characterized by an effective Poisson intensity $\lambda_{i,k}$ and a reward rate b_k, both of which depend on the contractual parameters (f_k, δ_k) whenever k corresponds to a pool. For a mining period normalised to $T = 1$, we model the payoff from venue k as a random variable $X_{i,k}$ with

$$\mathbb{E}[X_{i,k}] = \lambda_{i,k} b_k, \qquad \mathrm{Var}(X_{i,k}) = \lambda_{i,k} b_k^2.$$

If the miner allocates a fraction $w_{i,k}$ of her hashrate to venue k, the corresponding position contributes $w_{i,k} X_{i,k}$ to total wealth. Assuming independence across venues, the miner's total reward is

$$X_i = \sum_{k=0}^{n} w_{i,k} X_{i,k},$$

so that

$$\mathbb{E}[X_i] = \sum_{k=0}^{n} w_{i,k}\, \mathbb{E}[X_{i,k}] = \sum_{k=0}^{n} w_{i,k} \lambda_{i,k} b_k,$$

and, using $\mathrm{Var}\Big(\sum_k w_{i,k} X_{i,k}\Big) = \sum_k w_{i,k}^2 \mathrm{Var}(X_{i,k})$ under independence,

$$\mathrm{Var}(X_i) = \sum_{k=0}^{n} w_{i,k}^2\, \mathrm{Var}(X_{i,k}) = \sum_{k=0}^{n} w_{i,k}^2 \lambda_{i,k} b_k^2.$$

The miner evaluates allocations according to a mean–variance criterion

$$J_i(w_i) = \mathbb{E}[X_i] - \gamma_i\, \mathrm{Var}(X_i),$$

with risk aversion parameter $\gamma_i \in (0, 1)$. Under the above specification, this becomes

$$J_i(w_i) = \sum_{k=0}^{n} w_{i,k} \lambda_{i,k} b_k - \gamma_i \sum_{k=0}^{n} w_{i,k}^2 \lambda_{i,k} b_k^2.$$

The miner's optimal allocation solves the constrained optimization problem

$$\max_{w_i \in \Delta^n} \left\{ \sum_{k=0}^{n} w_{i,k} \lambda_{i,k} b_k - \gamma_i \sum_{k=0}^{n} w_{i,k}^2 \lambda_{i,k} b_k^2 \right\}, \tag{7}$$

where Δ^n denotes the n-dimensional unit simplex.

This modeling choice produces an endogenous hashrate supply for each pool,

$$H_k(f_k, \delta_k) = \sum_i \lambda_i\, w_{i,k},$$

which responds smoothly to contractual parameters (f_k, δ_k). Hence, pool managers face a continuously adjusting population of miners whose participation intensities shift in response to the risk–return characteristics encoded in the pools' contracts.

3.2 Pool Manager's mean-variance trade-off

For a given time horizon $T \geq 0$, the expected wealth of the pool manager associated to wealth process (4) is given by

$$\mathbb{E}(Y_t) = y + \mu t \, \frac{b\delta}{1+\delta}\Big(f(1+\delta) - \delta\Big). \tag{8}$$

and the variance of the wealth is given by

$$\mathrm{Var}(Y_t) = \mu t \left[\frac{b^2(1-f)^2\delta^2}{1+\delta} + \frac{b^2\delta\Big(1-(1-f)\delta\Big)^2}{1+\delta} \right]. \tag{9}$$

The pool manager seeks to maximize a mean–variance criterion of expected wealth,

$$J_{\text{mana}} = \mathbb{E}[Z_T] - \eta \, \mathrm{Var}[Z_T], \tag{10}$$

where $\eta \in (0,1)$ denotes the risk aversion coefficient of the pool manager. Using (18) and (19) and letting $T = 1$, this yields the objective function

$$J_{\text{mana}} = y + \mu \frac{b\delta}{1+\delta} \left[f(1+\delta) - \delta - \gamma b \Big(\delta(1-f)^2 + \Big(1-(1-f)\delta\Big)^2 \Big) \right]. \tag{11}$$

3.3 Miner Participation as Follower Reaction

For any contractual pair (f, δ), some miners will join the pool while the others mine solo according to their mean-variance criteria. The aggregate Hashrate contributed by entering miners is therefore

$$H_k(f,\delta) = \sum_i \lambda_i \, w_{i,k}, \tag{12}$$

and the induced share-arrival intensity of the surplus process is

$$\mu(f,\delta) = \frac{H(f,\delta)}{\delta}. \tag{13}$$

Hence, the pool manager's objective function becomes

$$J_{\text{mana}} = y + H(f,\delta) \frac{b\delta}{\delta(1+\delta)} \left[f(1+\delta) - \delta - \gamma b \Big(\delta(1-f)^2 + \Big(1-(1-f)\delta\Big)^2 \Big) \right]. \tag{14}$$

3.4 Nash Equilibrium in the Pool Market

3.4.1 Game Formulation

The interaction between pool managers constitutes a non-cooperative game. As established in Section 3.1, a miner i determines their optimal weight vector w_i^* by solving the optimization problem (7), which considers the characteristics of all available pools simultaneously. Consequently, the aggregate hashrate H_k collected by a pool k is not intrinsic to that pool but depends on the entire vector of contracts offered in the market.

Let n be the number of competing mining pools. We denote the strategy of manager k as the pair $s_k = (f_k, \delta_k)$. The strategy space $\mathcal{S}_k$ for each manager is constrained by the domain of validity for the parameters (typically $f_k \in [0,1]$ and $\delta_k > 0$) and the drift condition derived in (6), ensuring the pool's solvency:

$$\mathcal{S}_k = \{(f, \delta) \in [0,1] \times \mathbb{R}_+^* \mid f(1+\delta) > \delta\}. \tag{15}$$

Let $\mathbf{s} = (s_1, \dots, s_n) \in \prod_{k=1}^n \mathcal{S}_k$ denote the strategy profile of all managers. We define $\mathbf{s}_{-k}$ as the strategy profile of all managers except k. The hashrate captured by pool k is explicitly a function of the collective strategy profile:

$$H_k(\mathbf{s}) = \sum_i \lambda_i w_{i,k}^*(\mathbf{s}), \tag{16}$$

where $w_{i,k}^*(\mathbf{s})$ is the optimal allocation of miner i given the market configuration $\mathbf{s}$.

Substituting this into the manager's objective function defined in (14), the payoff for manager k, denoted $\mathcal{J}_k$, depends on their own strategy s_k and the strategies of competitors $\mathbf{s}_{-k}$:

$$\mathcal{J}_k(s_k, \mathbf{s}_{-k}) = \mathbb{E}[Z_T] - \eta_k \mathrm{Var}[Z_T], \tag{17}$$

where the moments are conditioned on the induced intensity $\mu(s_k, \mathbf{s}_{-k}) = H_k(s_k, \mathbf{s}_{-k})/\delta_k$.

We seek a Nash Equilibrium, representing a stable state of the network where no pool manager has an incentive to unilaterally deviate from their chosen contract parameters.

Definition 1 (Nash Equilibrium). A strategy profile $\mathbf{s}^* = (s_1^*, \dots, s_n^*)$ is a Nash Equilibrium if, for every manager $k \in \{1, \dots, n\}$ and any admissible strategy $s_k \in \mathcal{S}_k$:

$$\mathcal{J}_k(s_k^*, \mathbf{s}_{-k}^*) \geq \mathcal{J}_k(s_k, \mathbf{s}_{-k}^*). \tag{18}$$

At equilibrium, the pair (f_k^*, δ_k^*) maximizes manager k's mean-variance utility given that all other pools play their optimal strategies. This results in a simultaneous optimization of f and δ across the network.

3.4.2 Numerical Resolution: Iterated Best Response

The procedure computes the optimal response of each manager to the current market state iteratively. Let $\mathbf{s}^{(t)}$ be the strategy profile at iteration t. The algorithm proceeds as follows:

1. **Initialization:** Set an initial valid profile $\mathbf{s}^{(0)}$.

2. **Iteration:** For each manager $k = 1, \dots, n$ at step $t+1$:

$$s_k^{(t+1)} = \arg\max_{s \in \mathcal{S}_k} \mathcal{J}_k\left(s, s_1^{(t+1)}, \dots, s_{k-1}^{(t+1)}, s_{k+1}^{(t)}, \dots, s_n^{(t)}\right). \tag{19}$$

   This step involves a grid search over the admissible space $\mathcal{S}_k$ to find the pair (f, δ) that maximizes the objective, recalculating the miners' aggregate hashrate H_k for each candidate pair.

3. **Termination:** The process repeats until the Euclidean distance between consecutive strategy profiles falls below a predefined tolerance ϵ: $\|\mathbf{s}^{(t+1)} - \mathbf{s}^{(t)}\| < \epsilon$.

Convergence of the IBR algorithm implies the existence of a pure strategy Nash Equilibrium. The resulting strategies (f_k^*, δ_k^*) provide the theoretical equilibrium fees and difficulty parameters, explaining the decentralization levels observed in the network through the resulting hashrate vector $(H_1, \ldots, H_n)$.]

Example 1. To illustrate the competitive dynamics derived in Section 3.4.2, we simulate a market consisting of $n = 2$ mining pools and $N = 20$ individual miners. The total network hashrate is normalized to $\lambda = 6.0$, distributed among miners according to a Dirichlet distribution ($\alpha = 1$). The block reward is set to $b = 3.125$. We solve for the Nash Equilibrium using the Iterated Best Response algorithm. The results are summarized in Table 1.

Parameter	**Pool 1**	**Pool 2**
Risk Aversion (η)	0.01	0.02
Fee (f^*)	0.106	0.114
Difficulty parameter (δ^*)	0.020	0.020
Resulting Hashrate (H)	3.33	2.30
Manager Utility ($\mathcal{J}$)	3.58	5.25

Table 1: Equilibrium strategies with heterogeneous pool managers.

The simulation reveals a distinct competitive behavior driven by risk preferences. Manager 1, having a lower risk aversion ($\eta_1 = 0.01$), adopts a lower fee ($f_1^* \approx 10.6\%$) compared to Manager 2 ($f_2^* \approx 11.4\%$). Consequently, Pool 1 captures a dominant market share. Note that while Manager 2 ends with a higher total utility ($\mathcal{J}_2 > \mathcal{J}_1$), this is largely driven by the higher initial endowment ($y_2 = 5$ vs $y_1 = 3$) rather than the mining operations themselves. Figure 1 illustrates the final allocation of computational power.

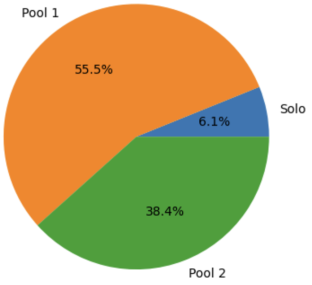

Figure 1: Equilibrium hashrate distribution.

To validate the robustness of the equilibrium found in Table 1, we examine the dynamic trajectory of the managers' strategies over the course of the simulation. Figure 2 plots the evolution of fees (f) and difficulty parameters (δ) for both pools over iterations of the Best Response algorithm.

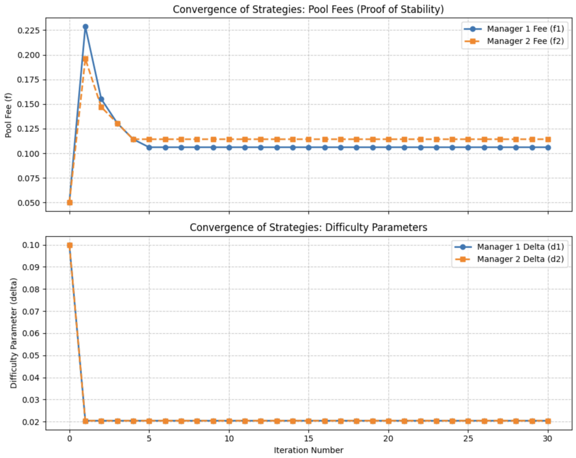

Figure 2: Convergence of pool strategies to demonstrates the attainment of a stable Nash Equilibrium without cyclical behavior.

As observed in the top panel, the fees adjust rapidly from their initial conditions to settle at their optimal levels ($f_1^* \approx 10.6\%$ and $f_2^* \approx 11.4\%$) within the first 6 iterations. Similarly, the bottom panel shows an immediate convergence of the difficulty parameters to the optimal lower bound $\delta^* \approx 0.02$. Crucially, the trajectories remain perfectly horizontal from iteration 6. This plot confirms that the strategy profile is a stable fixed point: neither manager has any incentive to deviate, even when the simulation is allowed to run for an extended period. This visual evidence rules out the existence of unstable cycles and validates the numerical precision of the Nash Equilibrium.

Acknowledgements

References