# Decentralized Mining in Centralized Pools*

Lin William Cong† Zhiguo He‡ Jiasun Li§

*First draft: March 2018. Current draft: August 2019.*

**Abstract**

The rise of centralized mining pools for risk sharing does not necessarily undermine the decentralization required for public blockchains. However, mining pools as a financial innovation significantly escalates the arms race among competing miners and thus increases the energy consumption of proof-of-work-based consensus mechanisms. Each individual miner's cross-pool diversification and endogenous fees charged by pools generally sustain decentralization — larger pools better internalize their externality on global hash rates, charge higher fees, attract disproportionately fewer miners, and thus grow slower. Empirical evidence from Bitcoin mining supports our model predictions, and the economic insights inform many other blockchain protocols, as well as the industrial organization of mainstream sectors with similar characteristics.

**JEL Classification:** D47, D82, D83, G14, G23, G28

**Keywords:** Arms Race, Bitcoin, Blockchain, Cryptocurrency, Energy Consumption, Industrial Organization, Mining Pools, PoW, Risk-Sharing.

*We thank Foteini Baldimtsi, Joseph Bonneau, Matthieu Bouvard, Bhagwan Chowdhry, Douglas Diamond, Hanna Halaburda, Wei Jiang, Evgeny Lyandres, Ye Li, Richard Lowery, Maureen O'Hara, George Panayotov, Fahad Saleh, Katrin Tinn, Liyan Yang, David Yermack, and Xin Wang for helpful discussions; Zhenping Wang, Xiao Yin, and Xiao Zhang provided excellent research assistance. We also thank seminar audiences at Ant Financial, Chicago, Cleveland Fed, Columbia, Cornell, CUNY Baruch, Duke, George Mason, Hong Kong University, Houston, Maryland, Michigan, NYU, Tsinghua PBC, Princeton, Rice, Stanford, UNC (Microeconomic Theory), Yale, as well as conference participants at Asian Development Bank Conference on FinTech, Becker Friedman Institute Conference on Cryptocurrencies and Blockchains, CEPR Gerzensee ESSFM Workshop, CIFFP, Credit and the Future of Banking Conference (Rigi Kaltbad), DataYes & ACM KDD China FinTech×AI Workshop, Econometric Society NA Meeting, ESSFM (Gerzensee), Georgia State FinTech Conference, Harvard CMSA Blockchain Conference, ISB Summer Conference, Midwest Finance Association Meeting, Northern Finance Association Meeting, SAIF Summer Institute, SFS Cavalcade Asia-Pacific, and 2nd Toronto FinTech Conference for helpful comments and discussions. This research was funded in part by the Ewing Marion Kauffman Foundation. The contents of this publication are solely the responsibility of the authors. We are also grateful for funding from the Center of Initiative on Global Markets, the Stigler Center, and the Center for Research in Security Prices at the University of Chicago Booth School of Business, and from the Multidisciplinary Research (MDR) Initiative in Modeling, Simulation and Data Analytics at George Mason.

†Cornell University SC Johnson College of Business. Email: will.cong@cornell.edu

‡University of Chicago and NBER. Email: zhiguo.he@chicagobooth.edu

§George Mason University. Email: jli29@gmu.edu

# 1 Introduction

Digital transactions traditionally rely on a central record-keeper, who is trusted to behave honestly and be sophisticated enough to defend against cyber-vulnerabilities. Blockchains instead decentralize record-keeping, with the best-known application being the P2P payment system Bitcoin (Nakamoto, 2008). The majority of existing blockchains rely on various forms proof-of-work (PoW) protocols, often known as "mining," in which independent computers ("miners") dispersed all over the world spend resources and compete repeatedly for the right to record new blocks of transactions, and the winner in each round gets rewarded.[1] Independent miners have incentives to honestly record transactions because rewards are valid only if their records are endorsed by subsequent miners.

Compared to a centralized system, a blockchain has several advantages, including enhanced robustness to cyber-attacks or mechanical glitches from the removal a "single point of failure."[2] A blockchain is also presumably less vulnerable to misbehaviors or censorships, as it shifts the trust on the stewardship of a central book-keeper to the selfish economic incentives of a large number of competitive miners. However, these advantages rely on adequate decentralization of the system, which is so far only a *technological* possibility rather than a guaranteed *economic* reality. Indeed, while Nakamoto (2008) envisions a perfect competition among independent computer nodes dispersed across the world, many cryptocurrencies have over the years witnessed a rise of "pooled mining" wherein miners partner together and share mining rewards, as opposed to "solo mining" wherein individual miners bear all idiosyncratic risks. Furthermore, the benefits of PoW blockchains come at high costs: practitioners and academics well-recognize their ever-increasing energy consumption and the climate and environmental consequences.[3]

Bitcoin mining provides an illustration: Mining pools grew from constituting only 5% of the global hash rates (a measure of computation power devoted to mining) in June 2011 to almost 100% ever since late 2015, as shown in Figure 1. The rise of mining pools also

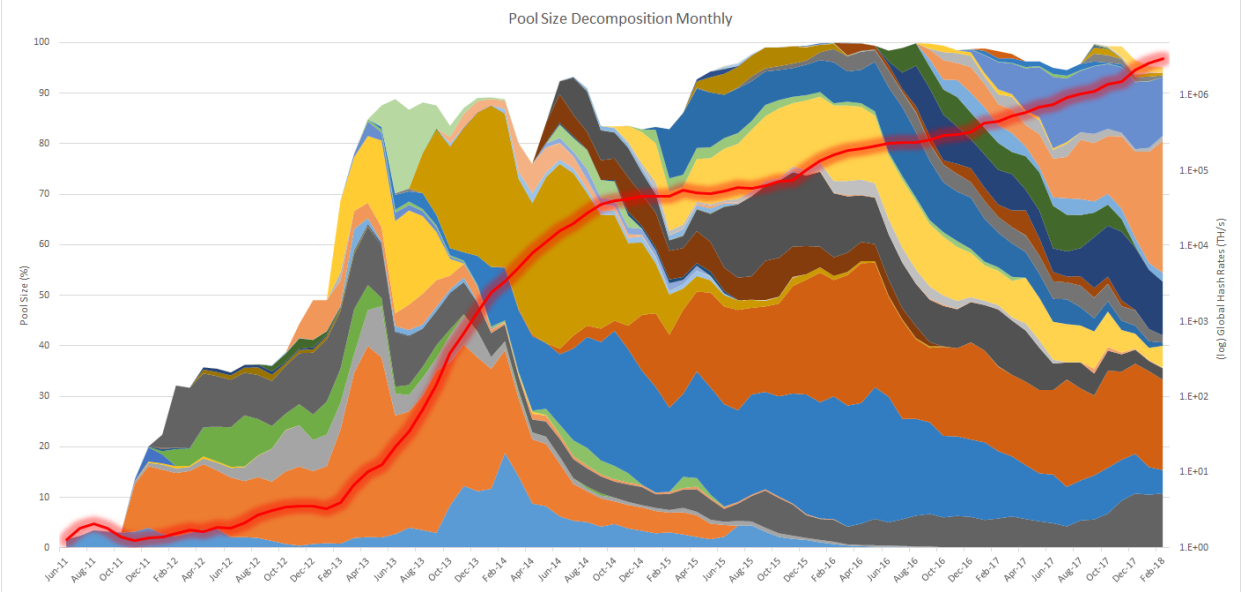
[1] Section 6.3 extends our discussion to other consensus protocols such as Proof-of-Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), etc.

[2] The recent scandal at Equifax offers a vivid lesson. See, e.g., Economist (2017).

[3] As of April 2018, aggregate electricity devoted to Bitcoin mining alone exceeds 60 TWh, roughly the annual energy consumed by Switzerland (Lee, 2018). The cryptocurrency forum Digiconomist provides similar estimates, noting that mining a single block consumes enough energy to power more than 28 U.S. homes for a full day (https://digiconomist.net/bitcoin-energy-consumption). Mora, Rollins, Taladay, Kantar, Chock, Shimada, and Franklin (2018) project that if Bitcoin follow the adoption pattern of other technologies, it could push global warming above 2 Celsius degrees within three decades. See also Rogers (2017).

Figure 1: **The evolution of size percentages of Bitcoin mining pools**

This graph plots (1) the growth of aggregate hash rates (right hand side vertical axis, in log scale) starting from June 2011 to today; and (2) the size evolutions of all Bitcoin mining pools (left hand side vertical axis) over this period, with pool size measured as each pool's hash rates as a fraction of global hash rates. Different colors indicate different pools, and white spaces indicate solo mining. Over time, Bitcoin mining has been increasingly taken over by mining pools, but no pool seems to ever dominate the mining industry for long. The pool hash rates data come from Bitcoinity and BTC.com, with details given in Section 5.




coincides with the explosive growth of global hash rates (plotted in red line, in log scale). Meanwhile, some pools gained significant shares from time to time, with the best-known example being GHash.io that briefly reached over 51% of global hash rates in July, 2014. Although such cases call into question whether a blockchain system can stay decentralized, none of the large pools emerged has snowballed into dominance for prolonged periods of time. Instead, Figure 1 reveals that pool sizes seem to exhibit a mean reverting tendency, suggesting concurrent economic forces suppressing over-centralization.

Motivated by these observations, we study the various centralization and decentralization forces in the creation and industrial organization of mining pools, and relate them to the energy consumption of mining as well as classic economic theories. Specifically, we model miners' decision-making in acquiring and allocating hash rates into mining pools, together with the competition among pool managers who charge fees for providing risk-sharing services. We highlight two features of cryptocurrency mining that are key to understanding our results: (i) It is easy for profit-driven miners to participate in multiple mining pools, an

interesting feature that contrasts with the traditional literature on labor and human capital in which each individual typically only holds one job; (ii) As explained shortly, the dynamic adjustment of mining difficulty needed to ensure network security leads to an arms race, imposing a negative externality that each individual's acquisition of hash rates directly hurts others' payoffs.

We first underscore the significant risk-sharing benefit offered by mining pools: under reasonable parameters, the certainty equivalent of joining a pool more than doubles that from solo mining. Absent other considerations, a larger pool also offers higher risk-sharing benefits. From an economist's perspective, these results are natural, as partnerships/cooperatives have been one of the most common organizational forms in humans history for risk sharing among individuals, and as in the insurance industry, risk sharing works better when the insurance provider covers a larger market. Yet in conventional settings the risk-sharing benefit is rarely separable from production technologies with increasing economy of scale. The production function of mining is such that the total revenue stays the same whether two miners join force or not, and hence implies that mining pools emerge primarily due to risk sharing, allowing us to pinpoint the interaction of risk sharing and competition.

While the above arguments may lead to a hasty conclusion that a large pool would grow even larger, we prove otherwise: In a frictionless benchmark, perfect risk sharing could be obtained and the exact pool size distribution is irrelevant. This is because the risk-sharing benefit *within* a large pool could be alternatively obtained through miner's diversification *across* multiple small pools — a general insight reminiscent of the Modigliani-Miller Theorem. Although investors (miners) are risk-averse, it is not necessary to have conglomerate firms (pools) for risk sharing purposes, as investors (miners) can diversify on their own in the financial market by holding a diversified portfolio (allocating hash rates to multiple pools). As a result, the folk wisdom in the blockchain community that pools become concentrated for better risk sharing is misguided, as long as miners can freely allocate their hash rates. In other words, risk sharing indeed leads to the rise of mining pools, but not necessarily further consolidations of pools (hence over-concentration).

Instead, the real consequence we emphasize is that the enormous amount of energy devoted to mining can be largely attributed to mining pools, which, as a financial innovation intended for better risk sharing, severely escalates the arms race within PoW blockchains. Under reasonable model parameters, mining pools can elevate the global computation power

devoted to mining by multiple times. Given that it is widely argued that cryptomining divert electricity and fossil fuel from other uses and detrimental environmental impacts (e.g., Benetton, Compiani, and Morse, 2019; Li, Li, Peng, Cui, and Wu, 2019; de Vries, 2019; Truby, 2018), our theory makes a timely contribution by pointing out for the first time that the organization of mining pools contribute significantly to global energy consumption, in addition to the usual suspect of rising cryptocurrency prices.

Building on the insights from the frictionless benchmark, we introduce an empirically relevant friction: some "passive hash rates," however small, are not always optimally allocated in real time, for example, due to miners' inattention. This friction introduces pool heterogeneity and potential market power, and allows us to better understand the industrial organization of mining pools observed in practice, as well as its impact on the mining arms race. We characterize the equilibrium in a static setting, and explain how the initial pool size distribution affects pool growth: A larger incumbent pool optimally charges a higher fee, which slows its percentage growth relative to smaller pools. In other words, if our model were dynamic, pool sizes mean-revert endogenously.

The central force behind this result is the arms race effect highlighted earlier: A larger pool has a larger impact on the global hash rates. As a result, a larger pool charges a higher fee and accommodates proportionally less active mining, in a similar spirit to traditional oligopolistic models where larger producers charge higher prices and produces less.[4] Consequently, absent other considerations, in the long run we expect a relatively decentralized market structure to sustain in the global mining industry, and no single pool grows too dominant. Note that the escalation of mining arms race and the benefit to miner's diversification across multiple pools are present with or without "passive hash rates," but the mean reversion in pool size relies on this friction.

Eempirical evidence from Bitcoin mining supports our theoretical predictions. Every quarter, we sort pools into deciles based on the start-of-quarter pool size, and calculate the average pool share, average fee, and average log growth rate for each decile. We find that pools with larger start-of-quarter size indeed charge higher fees, and grow slower in percentage terms. We investigate these relationship in three two-years windows (i.e., 2012-2013,

[4]Nevertheless, the interaction of risk-sharing externality (a form of economy of scale) of a pool, diversification across pools, and pool owners' local monopolistic power also distinguishes our model from earlier theoretical models such as Salop and Stiglitz (1977); Varian (1980), which does not feature economy of scale and stores charging higher prices only attract uninformed consumers (similar to our passive miners).

2014-2015, and 2016-2017) respectively, and find in every window statistically significant results with signs predicted by our theory.[5] We also discuss alternative channels and why the ones we highlight are likely important drivers.

In addition to the cross-section evidence on pool size, pool fees, and pool growth, we also note that the rise of mining pools indeed coincides with the explosion of global hash rates.[6] Under reasonable parameters, we find that in equilibrium the encouragement of more hash rate acquisition induced by risk sharing trumps the discouragement from pool fees, and the presence of mining pools still significantly amplifies mining energy consumption.

We further discuss several robustness results: taking into account pool entry as in a contestable market, introducing aggregate risks, and applying the model insights to alternative proof-of-work or proof-of-stake protocols. We also discuss how other external forces that counteract over-concentration of pools could be added onto our framework.

**Related literature.** Our paper contributes to emerging studies on blockchains and distributed ledger systems (e.g., Harvey, 2016).[7] Specifically, our study directly relates to cryptocurrency mining games. Adding to earlier studies of Nakamoto (2008), Kroll, Davey, and Felten (2013), and Kiayias, Koutsoupias, Kyropoulou, and Tselekounis (2016), Biais, Bisiere, Bouvard, and Casamatta (2018) analyze equilibrium multiplicity in cryptocurrency mining. Easley, O'Hara, and Basu (2017) and Huberman, Leshno, and Moallemi (2017) relate transaction fees to mining and user waiting times. Dimitri (2017) and Ma, Gans, and Tourky (2018) model mining as a Cournot-type competition and R&D race. Prat and Walter (2018) examine the relationship between Bitcoin price and hash rate investment. Many

[5]These empirical patterns on the size-fee and size-growth relationships in the burgeoning Cryptocurrency industry should not be taken granted. In the passive asset management industry which offers index funds to retail investors, a larger fund actually charges lower fees; Hortaçsu and Syverson (2004) provides a search-based mechanism to explain this empirical regularity. Furthermore, although earlier studies on the size-growth relation indeed document that larger firms grow less (Caves, 1998; Rossi-Hansberg and Wright, 2007), the recent literature on ''superstar" firms finds increasing concentrations in the past decades across various industries, and hence a positive size-growth relationship (Autor, Dorn, Katz, Patterson, and Van Reenen, 2017; Andrews, Criscuolo, Gal, et al., 2016)

[6]No causality claimed, as other factors could have also contributed to the explosion of global mining power in Figure 1, such as upgrades of mining hardwares, increasing awareness of mining, etc.

[7]Other studies include Cong and He (2018) that examines informational tradeoffs in decentralized consensus generation and how they affect business competition. Several papers study the impact of blockchains on corporate governance (Yermack, 2017), holding transparency in marketplaces (Malinova and Park, 2016), security-trade settlements (Chiu and Koeppl, 2018), and financial reporting and auditing (Cao, Cong, and Yang, 2018). Also related are studies on initial coin offerings for project launch (Li and Mann, 2018), as well as cryptocurrency valuation and the roles of tokens on platform adoption (Cong, Li, and Wang, 2018).

studies also reveal that an adequate level of decentralization is crucial for the security of a blockchain.[8] For example, Eyal and Sirer (2014) and Eyal (2015) study "selfish mining" and miner's dilemma in which miners launch block-withholding attacks.[9]

These papers often follow the convention in the computer science literature to only consider one pool behaving strategically as a single decision-maker.[10] Moreover, almost all of them only consider risk-neutral miners and take any mining pools as exogenously given singletons, while we emphasize risk-aversion — the rationale behind the emergency of mining pools in the first place. In contrast, we characterize the full equilibrium wherein both miners and pools are strategic and risk-averse, in addition to modeling the incentives of participants and managers within each pool. Our findings on the creation and distribution of mining pools also connect with strands of literature on contracting and the theory of the firm.[11] Instead of focusing on a single pool as in Rosenfeld (2011); Schrijvers, Bonneau, Boneh, and Roughgarden (2016); Fisch, Pass, and Shelat (2017), we analyze the contracting relationships among miners and pool managers and the interaction of multiple pools in an industrial organization framework.

Many blogs, think tank reports, and media article have taken notice of the large energy consumption by cryptocurrency mining. They focus on Bitcoin prices and mining hardwares (e.g., ASICs versus GPUs, see Kugler, 2018), rather than modeling the mining industry and identifying the impact from mining pools, which could be equally important. Several studies recognize that costly mining serves to enhance network security and prevent double spending (e.g. Chiu and Koeppl, 2017; Budish, 2018; Pagnotta and Buraschi, 2018); some also point out the social waste from high energy consumption by cryptocurrency mining in its current form (e.g. Chiu and Koeppl, 2017; Saleh, 2017). We are the first to demonstrate how risk sharing affects the organization and energy consumption of the mining industry.[12]

[8] Nakamoto (2008) explicitly requires that no single party shall control more than half of global computing power for Bitcoin to be well-functioning (thus the concept of 51% attack). Empirically, Gencer, Basu, Eyal, van Renesse, and Sirer (2018) investigate the extent of decentralization by measuring the network resources of nodes and the interconnection among them. Also related is Budish (2018), which suggests intrinsic economic limits to how economically important Bitcoin can become before being subjected to majority attacks.

[9] Along this line of research, Sapirshtein, Sompolinsky, and Zohar (2015) develop an algorithm to find optimal selfish mining strategies. Nayak, Kumar, Miller, and Shi (2016) (stubborn mining) goes beyond the specific deviation in Eyal and Sirer (2014) and consider a richer set of possible deviating strategies. They conclude that there is no *one-size-fits-all* optimal strategy for a strategic miner.

[10] Beccuti, Jaag, et al. (2017) is an exception on how miner number/heterogeneity affects block-withholding.

[11] Classical studies include Wilson (1968) on syndicates and Stiglitz (1974) on sharecropping. Recent studies include Li (2015) on private information coordination.

[12] Our insight also shows up in traditional financial markets. For example, Li (2017) similarly features

The novel economic forces we identify in the mining industry also closely relate to classic economic theories. In addition to the theory of the firms, the Modigliani-Miller insight, and oligopoly pricing as discussed earlier, active miners' hash rate allocation decisions shares the spirit of investors' capital allocation decisions to mutual funds as in Berk and Green (2004). The arms race nature of crypto-mining is also related to research on arms race in finance, notably Glode, Green, and Lowery (2012). Instead of emphasizing how the arms race can destroy value beyond the resources invested directly through adverse selection, we focus on how a financial innovation for risk sharing can exacerbate the arms race. The hard-coded nature of a blockchain together with its transparency offers researchers a unique social science laboratory for analyzing and testing economic theories, for example, on risk sharing and competition, without the complication of agency issues.[13] We elaborate on these points further in Section 2.6.

The rest of the paper proceeds as follows. Section 2 introduces the institutional details of PoW mining and stylized facts about mining pools. Section 3 sets up the model and analyzes a frictionless benchmark. Section 4 characterizes the equilibrium. Section 5 provides corroborating empirical evidence using Bitcoin data, before Section 6 discusses broader implications and extensions. Section 7 concludes.

# 2 Mining Pools: Background and Principle

This section provides background knowledge of the Bitcoin mining process, analyzes the risk-sharing benefit of mining pools, and introduces typical pool-fee contracts. Mining in other PoW blockchains operates similarly.

## 2.1 Mining and Risky Reward

Bitcoin mining is a process in which miners around the world compete for the right to record a brief history (known as block) of bitcoin transactions. The winner of the competition is rewarded with a fixed number of bitcoins (currently 12.5 bitcoins, or ₿12.5), plus any transactions fees included in the transactions within the block.[14] In order to win the

better risk sharing leading to more aggressive risk.

[13]The arms race nature is also related to the long literature of contests and rent seeking (Nitzan, 1991; Konrad, 2007). The key difference here is the absence of moral hazard due to the observability of effort.

[14]See Easley, O'Hara, and Basu (2017) and Huberman, Leshno, and Moallemi (2017) for more details.

competition, miners have to find a piece of data (known as solution, or nonce), so that the hash (a one-way function) of the solution and all other information about the block (e.g. transaction details within the block and the miner's own bitcoin address) has an adequate number of leading zeros. The minimal required number of leading zeros determines the mining difficulty.

Under existing cryptography knowledge, the solution can only be found by brute force (enumeration). Once a miner wins the right to record the most recent history of bitcoin transactions, the current round of competition ends and a new one begins.

Technology rules that for all practical purposes the probability of finding a solution is not affected by the number of trials attempted. This well-known memoryless property implies that the event of finding a solution is captured by a Poisson process with the arrival rate proportional to a miner's share of hash rates globally (e.g., Eyal and Sirer, 2014; Sapirshtein, Sompolinsky, and Zohar, 2016). Specifically, given a unit hash cost $c$ and a dollar award $R$ for each block, the payoff to a miner who has a hash rate of $\lambda_A$ operating over a period $T$ is

$$X_{solo} - c\lambda_A T, \text{ where } X_{solo} = \tilde{B}_{solo} R \text{ with } \tilde{B}_{solo} \sim \text{Poisson}\left(\frac{1}{D}\frac{\lambda_A}{\Lambda}T\right). \tag{1}$$

Here, $\tilde{B}_{solo}$ is the number of blocks the miner finds within $T$ — a Poisson distributed random variable capturing the risk that a miner faces in this mining game. $\Lambda$ denotes global hash rate (i.e., the sum of hash rates employed by all miners, whether individual or pool), $D = 60 \times 10$ is a constant so that on average one block is created every 10 minutes.

The hash cost $c$ in Eq.(1) is closely related to the energy used by computers to find the mining solution. More importantly, an individual or pool's success rate is scaled by the global hash rate $\Lambda$ devoted to mining, capturing the dynamic adjustment of the mining difficulty so that one block is delivered per ten minutes on average.[15] As emphasized later, this constitutes the driving force for the mining "arms race" with negative externality.

Because mining is highly risky, any risk-averse miner has strong incentives to find ways to reduce risk.[16] A common practice is to have miners mutually insure each other by forming

[15]This dynamic adjustment for scaling miners' winning probabilities is a common feature in both PoW and PoS blockchains. It ensures network security and reduces block collision (Gervais, Karame, Wüst, Glykantzis, Ritzdorf, and Capkun, 2016; Vukolić, 2015).

[16]Bitcoin mining is in some sense analogous to gold mining. Just like a gold miner who spends manpower and energy to dig the ground in search of gold, a Bitcoin miner spends computing powers and related electricity/cooling/network expenses in search of solutions to some cryptography puzzles; just like a gold miner who only gets paid when he successfully finds the gold, a Bitcoin miner only gets paid when he finds

a (proportional) mining pool. The next section describes how such a mining pool works.

## 2.2 Mining Pool and Risk Sharing

A mining pool combines the hash rates of multiple miners to solve one single cryptographic puzzle, and distributes the pool's mining rewards back to participating miners in proportion to their hash rate contributions.[17] The initiation process of a pool typically starts with the pool manager coming up with the hardware infrastructure, followed by programming the necessary codes that implement the operations and compensations of the pools, and then marketed to the miner community. Some mining pools were initiated by corporations, as in the case of the largest mining pool currently, AntPool, which was created by Bitmain Inc.

Ignoring fees that represent transfers among pool members for now, then following the previous example, the payoff to a participating miner with hash rate $\lambda_A$ who joins a pool with existing hash rate $\Lambda_B$ (throughout we use upper case $\Lambda_m$ to indicate hash rates at the pool level) is

$$X_{pool} - c\lambda_A T, \text{ where } X_{pool} = \frac{\lambda_A}{\lambda_A + \Lambda_B}\tilde{B}_{pool}R \text{ with } \tilde{B}_{pool} \sim \text{Poisson}\left(\frac{\lambda_A + \Lambda_B}{\Lambda}\frac{T}{D}\right). \quad (2)$$

Pooled mining provides a more stable cash flow and reduces the risk a miner faces. Indeed,

**Proposition 1** (Risk Sharing Dominance)**.** *$X_{pool}$ second-order stochastically dominates $X_{solo}$, so any risk-averse miner strictly prefers $X_{pool}$ over $X_{solo}$.*

For illustration, consider the symmetric case with $\lambda_A = \lambda_B$. Relative to solo mining, a miner who conducts pooled mining is twice likely to receive mining payouts but half the rewards at each payment, generating a standard risk-sharing benefit.

While the risk-sharing benefit manifests itself in traditional industries too, it is often inseparable from technologies with increasing economy of scale that naturally lead to industry concentration. For example, in gold mining, even risk-neutral miners would join force to reduce overheads and duplicate effort. Mathematically, given a production function $F(\cdot)$,

a solution. Both are risky – a miner could continuously expend resources mining for a prolonged period without any pay in the absence of a solution.

[17] Because the number of candidate partial solutions is astronomical, it makes negligible difference to each participating miner's payoff whether the pool coordinates their mining efforts or simply randomize the assignment of partial problems.

$F(x_1 + x_2) > F(x_1) + F(x_2)$, where $x_1$ and $x_2$ are inputs of two firms/individuals. Crypto-mining is unique in the sense that there is no mechanical economy of scale because the aggregate speed of building blocks is set by the protocol. Block generation follows a Poisson arrival given the current cryptography technology and difficulty adjustments. The additive property of Poisson processes in turn implies the total revenue stays the same whether two miners join force or not, that is, $F(x_1 + x_2) = F(x_1) + F(x_2)$. The setting therefore allows us to isolate and test the effects of pure risk sharing.

## 2.3 Quantifying the Risk-Sharing Benefits of Pooled Mining

The risk-sharing benefits of joining a mining pool can be substantial. To assess the magnitude, we calculate the difference of certainty equivalents of solo mining and pooled mining for a typical miner. Throughout the paper we use preference with Constant Absolute Risk Aversion (CARA), i.e., exponential utility with risk-aversion parameter $\rho$:

$$u(x) \equiv \frac{1}{\rho}\left(1 - e^{-\rho x}\right). \tag{3}$$

All quantitative implications of our model will be calibrated based on widely-accepted magnitudes of Relative Risk-Aversion (CRRA) coefficient.

The certainty equivalent of the revenue from solo mining, $CE_{solo}$, can be computed as

$$CE_{solo} \equiv u^{-1}(\mathbb{E}[u(\tilde{X}_{solo})]) = \frac{\lambda_A}{\Lambda}\frac{1}{\rho}\left(1 - e^{-\rho R}\right)\frac{T}{D}. \tag{4}$$

Similarly, the certainty equivalent of the revenue from joining a mining pool, $CE_{pool}$, is

$$CE_{pool}\left(\Lambda_B\right) \equiv u^{-1}(\mathbb{E}[u(\tilde{X}_{pool})]) = \frac{(\lambda_A + \Lambda_B)}{\Lambda}\frac{1}{\rho}\left(1 - e^{-\rho R\frac{\lambda_A}{\lambda_A + \Lambda_B}}\right)\frac{T}{D}. \tag{5}$$

We highlight that this certainty equivalent depends on the pool size $\lambda_B$ and typically a larger pool offers greater risk sharing benefit.

We choose reasonable parameters to gauge the magnitude of the risk-sharing benefit of joining a pool. Suppose $\lambda_A = 13.5$(TH/s), which is what one Bitmain Antminer S9 ASIC miner (a commonly used chip in the Bitcoin mining industry) can offer; $\Lambda_B = 3,000,000$(TH/s), which is at the scale of one large mining pool; $R = \$100,000$ (฿12.5 reward + ∼฿0.5 transaction fees per block and \$8000 per BTC gives \$104,000); $\Lambda =$

$21,000,000$(TH/s), which is the prevailing rate; and $\rho = .00002$ (assuming a CRRA risk aversion of 2 and a wealth of \$100,000 per miner gives a corresponding CARA risk aversion of 0.00002). Take $T = 3600 \times 24$ which is one day. Then $CE_{solo} = 4.002$ and $CE_{pool} = 9.257$, which implies a difference of 5.255, about 57% of the expected reward $\mathbb{E}(\tilde{X}_{solo})$ (about 9.257). In other words, for a small miner, joining a large pool almost boost his risk-adjusted payoff by more than 131%.[18] Equally relevant, for more risk-averse miners (e.g. $\rho = .00004$), given the current mining cost parameters, joining a pool could turn a (certainty equivalent) loss into a profit.[19]

The risk-sharing benefit has two major implications. First, active miners with a given level of risk aversion would acquire hash rates more aggressively when mining in pools, which escalates mining arms race and amplifies the energy consumption associated with cryptocurrency mining. Second, mining pools could charge fees (price) to miners, which in turn determine miners' optimal hash rates allocations (quantity). Before we develop a model to study the equilibrium fees and allocations under mining pool competitions, we first describe the various forms of fee contracts used in practice.

## 2.4 Fee Contracts in Mining Pools

Broadly speaking, different pools in practice offer three categories of fee contracts: *Proportional*, *Pay per Share* (PPS), and *Cloud Mining*. Table 3 in Appendix B gives a list of contracts currently used by major pools. As explained later, all contracts effectively have the same contracting variable – participating miners' hash rates, and the three categories mainly differ in two aspects: (i) the mapping from the contracting variable to payoff, and (ii) pool fees and the treatment of transaction fees. We proceed to describe the contracting variables and compare the mappings from contracting variables to payoffs. Other technical

[18] Even if we set $\rho = .00001$ (a miner with CRRA risk aversion of 2 and is twice richer), joining this large pool increases his risk-adjusted payoff by more than 85%. The risk-sharing benefit can be still quantitatively large even for small pools. For a small mining pool with only one existing miner using a S9 ASIC chip so that $\Lambda_B = 13.5$, joining it still implies a difference in certainty equivalents about 20% of the reward. All values above were chosen at the time when the paper was first written in early 2018, including the Bitcoin price \$8,000. The risk-sharing benefit remains large even with a much lower Bitcoin price, which is \$3,600 around early 2019. When we replace \$8,000 with \$3,600, for a small miner joining a large pool almost boost his risk-adjusted payoff by more than 52%.

[19] Assuming a \$0.12 per kWh electricity cost, and 1375w/h for S9 (see here), the power consumption is $c = 1.375 \times 0.12/(3600 \times 13.5)$ per TH. Then $\frac{1}{D\rho}\frac{\lambda_A+\Lambda_B}{\Lambda}\left(1 - e^{-\rho R\frac{\lambda_A}{\lambda_A+\Lambda_B}}\right) - \lambda_A C = \$6.1 \times 10^{-5}$/s or \$5.3/day, while $\frac{1}{D\rho}\frac{\lambda_A}{\Lambda}\left(1 - e^{-\rho R}\right) - \lambda_A C = -\$2.0 \times 10^{-5}$/s or $-\$1.7$/day.

details are left out as they are not essential for understanding the rest of the paper.

**Pool managers and mining reward.** A mining pool is often maintained by a pool manager, who takes a percentage cut from miners' rewards at payout, known as pool fees which differ across pool contracts. In practice, when contributing to the same pool under the same contract, all miners are subject to the same pool fee, regardless of the amount of hash rates they contribute. In other words, there is no price discrimination.

Furthermore, different pools also vary in how they distribute transaction fees in a block. These transaction fees are different from the pool "fees" that we focus on; as discussed in Section 2.1, the transaction fees are what Bitcoin users pay to miners for including their intended transactions into the newly mined block. While most pools keep transaction fees and only distribute the fixed rewards from new blocks, given the recent rise of transaction fees more pools now also share transactions fees. Our reduced form block reward $R$ encompasses both types of rewards.

**Effectively observable hash rates.** All classes of fee contracts effectively use a miner's hash rate as a contracting variable. Although in theory a miner's hash rate is unobservable to a remote mining pool, computer scientists have designed ways to approximate it with high precision by counting so-called partial solutions. A partial solution to a cryptographic puzzle, like a solution itself, is a piece of data such that the hash of all information about the block and the partial solution has at least an adequate number of leading zeros that is smaller than the one required by a full solution. One can view partial solutions as "trials," while the solution "the successful trial." Counting the number of partial solutions hence amounts to measuring hash rates with some measurement error.

Crucially, the approximation error between the measured hash rate and the true hash rate can be kept arbitrarily small with little cost.[20] For economists, if one interpret "mining" as "exerting effort," then an important implication is that the principal (pool manager) can measure the actual hash rate (miner's effort) in an arbitrarily accurate way, rendering moral hazard issues irrelevant. All team members' effort inputs are perfectly observable and contractible, and the only relevant economic force is risk sharing, in stark contrast to that in Hölmstrom (1979).

[20]Different contracts may use different partial solutions or weigh them differently, while all give fairly accurate approximations of a miner's actual hash rate.

**Fee contracts.** As mentioned, the more than 10 types of fee contracts fall into three categories: proportional, pay per share (PPS), and cloud mining.

One predominant category entails proportional-fee contracts.[21] Under these contracts, each pool participant only gets paid when the pool finds a solution. The pool manager charges a fraction $f \in (0,1)$ of the block reward $R$, and then distributes the remaining reward $(1-f)R$ in proportion to each miner's number of partial solutions found (and hence proportional to their actual hash rates). More specifically, the payoff of any miner with hash rate $\lambda_A$ joining a pool with an existing hash rate $\lambda_B$ and a proportional fee $f$ is

$$\frac{\lambda_A}{\lambda_A+\Lambda_B}(1-f)\tilde{B}R - c\lambda_A T, \text{ with } \tilde{B} \sim \text{Poisson}\left(\frac{\lambda_A+\Lambda_B}{\Lambda}\right)\frac{T}{D}. \tag{6}$$

Another popular category entails pay-per-share (PPS) contracts: each pool participant gets paid a fixed amount immediately after finding a partial solution (again, in proportional to the hash rate). Hence the PPS contract corresponds to "hourly-based wages;" or, all participating miners renting their hash rates to the pool. Following the previous example, given a PPS fee $f_{PPS}$, the participating miner's payoff is simply $r \cdot \lambda_A$ with

$$r = \frac{RT}{D\Lambda}(1-f_{PPS}) \tag{7}$$

being the rental rate while giving up all the random block reward. As shown, in practice the PPS fee is quoted as a fraction of the expected reward per unit of hash rate (which equals $\frac{R}{\Lambda}\frac{T}{D}$). Cloud mining, which essentially makes miners rent hash rates from the pool, does exactly the opposite: a miner pays a fixed amount upfront to acquire some hash rate from the pool, and then gets paid as if conducting solo mining.

Our theory focuses on proportional fees only, though the analysis easily extends to the case of hybrid of proportional and PPS fees. There are two reasons for our modeling choice. First, in practice, about 70% of pools are adopting proportional fees, and 28% pools are using proportional fees exclusively.

[21] In practice, the most common proportional contract is Pay-Per-Last-N-Shares (PPLNS), which counts each pool participant's share within the last $N$ partial solutions submitted by all pool participants, instead of within the total number of partial solutions submitted in a given round before the pool finds a block. Other contracts that fall under the proportional category may discount partial solutions submitted long before the next block is found (e.g. as in geometric method). These alternative methods are adopted to prevent pool-hopping, a point important in practice yet irrelevant to our analysis, as all these methods approximates each pool participants' pay share according to her actual hash rate share.

Table 1: **Evolution of Pool Sizes and Fees**

This table summarizes the evolution of mining pool sizes and fees from 2011 to 2017. We report total hash rates in Column A, total number of mining pools in Column B, and in Column C the fraction of hash rates contributed by top-5 pools (i.e., sum of the top five pools hash rates over the market total hash rates, including those from solo-miners). In Column D, we report the average fee weighted by hash rates charged by mining pools. In Column E, we report the fraction of mining pools that use proportional fees; the fraction is calculated as the number of pools that use proportional fees divided by the number of pools with non-missing information on fee contracts. Column F and G give the simple averages of proportional fees and average total fees charged by top-5 pools, respectively; and Column H and Column I are simple averages across all pools. The pool hash rates information comes from Bitcoinity and BTC.com. The fee contract information is obtained from Bitcoin Wiki. All fee and size data are downloaded in Feb 2018 and converted into quarterly averages. Reward types are determined at the end of each quarter. Over time more hash rates are devoted to Bitcoin mining, and a majority of mining pools offer proportional contracts. The largest five pools on average charge higher fees.

| Year | Hash Rate (PH/s) (A) | # of Pools (B) | Top 5 (%) (C) | Avg. Fee (Size-Weighted) (%) (D) | # Frac. Of Prop. Pools (%) (E) | Fee (%) | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | Top 5 | | All | |
| | | | | | | Prop. (F) | Ave. (G) | Prop. (H) | Ave. (I) |
| 2011 | 0.01 | 8 | 7.63 | 0.57 | 87.12 | 0.28 | 0.28 | 0.28 | 0.25 |
| 2012 | 0.02 | 15 | 34.66 | 2.71 | 61.25 | 0.66 | 1.76 | 0.65 | 1.56 |
| 2013 | 1.48 | 23 | 71.01 | 2.73 | 62.57 | 1.58 | 2.29 | 1.16 | 2.02 |
| 2014 | 140.78 | 33 | 70.39 | 0.88 | 70.50 | 1.33 | 1.13 | 0.88 | 2.38 |
| 2015 | 403.61 | 43 | 69.67 | 1.51 | 77.92 | 1.10 | 1.31 | 0.84 | 1.33 |
| 2016 | 1,523.83 | 36 | 75.09 | 2.50 | 77.14 | 1.48 | 2.15 | 0.97 | 1.67 |
| 2017 | 6,374.34 | 43 | 62.25 | 1.67 | 78.89 | 2.00 | 1.43 | 1.42 | 1.32 |

The second reason, which is conceptually more important, is that a pure form of PPS or cloud mining only involves risk allocation between miners and pool manager. Under our framework with homogeneous risk aversion among miners and pool managers, they gain nothing adopting PPS or cloud mining. In contrast, a proportional fee contract provides risk sharing benefits.

## 2.5 Stylized Facts about Mining Pools

Table 1 provides an overview of the mining industry. The total hash rates in Bitcoin mining (Column $A$), the number of identified mining pools (Column $B$), as well as the concentration of mining pools (Column $C$, the total market share of the top-5 pools sorted by hash rates) have mostly been increasing since 2011. From an individual miner's perspective,

Column $D$ gives the average pool fee (including proportional, PPS, and others) weighted by hash rates for each year, which offers a gauge of overall cost in joining mining pools. Column E gives the fraction of hash rates in the mining pools that are using proportional fees; following a peak of 87% in 2011, this fraction has been mostly increasing in recent years, with about 79% in 2017.

The rest of four columns focus on the evolution and magnitude of pool fees which fall in the range of a couple of percentage points. Column $F$ and $G$ are for top-5 pools while Column $H$ and $I$ for all pools. The stylized fact revealed by comparing "Top 5" and "All" is that fees charged by top 5 pools are higher than the average fees charged by pools with all sizes. This is one salient empirical pattern that motivates our paper.[22]

## 2.6 Uniqueness about the Crypto-mining Industry

From the aforementioned institutional background, it should be apparent that there are a few unique features to the crypto-mining industry as compared to other traditional industries. We summarize them here.

First, while agents in traditional industries or employment relationship can decide how much effort and input to provide, they rarely can work for multiple firms at the same time (the concept of diversification). The rise of blockchains (as well as platforms such as Uber that facilitate sharing economy and on-demand labor) gives a setting where labor diversification manifests itself in a most transparent way.

Moreover, even when agents labor input (hash power in our case) can be fully diversified, traditional industries typically feature economy of scale in a mechanical way. For example, traditional gold mining firms enjoy economy of scale because they can maintain better relationship with banks and regulators. In the crypto-mining industry there is almost nothing mechanical about the economy of scale, risk-sharing is the primary driver in the settings we examine. In that sense, mining pools presents an environment where we can better isolate the impact or risk-sharing.

Last but not least, whereas in traditional contracting environment (labor contract), one has to worry about agency issues such as shirking, mining pools can very closely measure

[22]Proportional fees are in general smaller than "average fee" which is the average of proportional fees, PPS fees, and others. The reason is simple: PPS contracts offer zero risk exposure to participating miners, so risk-averse miners are willing to pay a higher PPS fee than that of proportional contracts (or equivalently, pool managers charge more from miners for bearing more risk).

effort inputs by counting partial solutions, and therefore are free of moral hazard.

Neglecting the above features often leads to many practitioners and policy-makers to hold beliefs that mining pools would eventually lead to over-concentration and dominance of a single pool. For example, some people are unaware that miners can allocate hash rates across pools. They argue that because in reality the aggregate hash power from individual miners that pools compete for is large, a larger pool would always charge a low enough fee to make miners join it rather than its rival. This would lead to a single pool dominating the entire industry.

# 3 An Equilibrium Model of Mining Pools

This section presents a model in which multiple pool managers compete in fees to attract active miners. We first derive a benchmark result: in a frictionless environment where all miners can actively acquire hash-rates and allocate them to different pools, risk sharing itself does not lead to centralization, simply because miners can diversify themselves across pools. The exact distribution of pool sizes also does not matter in this case.

Pool size distribution starts to matter when larger pools also have more passive hash rates that are not necessarily optimally allocated across pools — a case we examine in Section 4. We derive that larger pools charge higher fees, leading to slower pool growth, and then confirm these key theoretical predictions in Section 5 with data from Bitcoin mining pools.

The presence of mining pools also induces an aggressive arms race: Mining pools as a form of financial innovation for risk sharing increases the global hash rates devoted to mining. To the extent that the security of a blockchain features diminishing marginal benefit to global hash rates (once above a certain threshold), this escalated arms race leads to energy wastes.

## 3.1 Agents and Economic Environment

We study a static model with both pool managers and individual miners having the same CARA utility function given in Eq.(3) and using proportional-fee contracts.

**Pool managers and passive mining.** There are $M$ mining pools controlled by different managers; we take these incumbent pools as given and study pool entry later in Section 6.1. Pool $m \in \{1, \cdots, M\}$ has $\Lambda_{pm} > 0$ ($p$ stands for passive mining) existing passive hash

rates that stick to these pools. In the case of Bitcoin, although it involves little cost to re-adjust hash rates allocations, inattention or lack of information could generate inertia that leads to passive mining.[23] Passive mining can be alternatively interpreted as "loyal fans" of the mining pool forum or early investors (e.g., Torpey, 2016). In practice, a significant portion of $\Lambda_{pm}$ may also belong to the pool manager himself, which can be incorporated by modifying the fee expression. Our theoretical analysis does not hardwire on any particular interpretation  any hash rates that do not actively reallocate at the beginning of the time period are part of passive hash rates.

Empirically, we link $\Lambda_{pm}$ to the initial pool size, under the assumption that a fixed fraction of miners do not adjust their hash rate contributions across pools. Passive hash rates come from miners who do not pay attention to changes in pool sizes or fees in real time.[24] As we explain in Section 5, the exact link between passive miners $\sum_m \Lambda_{pm}$ and the initial pool size is not crucial for our qualitative results in the sense that in reality, pools of larger initial size have more passive mining but not disproportionally more, and as long as that is the case, our theoretical predictions are falsifiable through our empirical tests.

Given the significant risk-sharing benefit to individual miners illustrated in Section 2, managers of pools $\{m\}_{m=1}^{M}$ post (proportional) fees $\{f_m\}_{m=1}^{M}$ simultaneously to attract $\Lambda_{am}$ active miners and maximize their expected utility, $\mathbb{E}\left[u(\tilde{B}_m f_m R)\right]$, which can be expressed using certainty equivalent as

$$\max_{f_m \in [0,1]} \frac{\Lambda_{am}(f_m) + \Lambda_{pm}}{\rho \Lambda(f_m, f_{-m})} \left(1 - e^{-\rho R f_m}\right). \tag{8}$$

It is worth emphasizing that when setting fees, the oligopolistic pool managers understand the impact of fee levels on the global hash rate $\Lambda$ and hence their own expected utility. In other words, pool owners partially internalize the arms-race externality.

**Active miners.** There is a continuum of active homogeneous miners of total measure $N$, each of whom can acquire hash rate with a constant unit cost $c$. In other words, while mining pools may enjoy market power, active miners are competitive.[25]

[23] See, for example, threads on the Bitcointalk forum at https://bitcointalk.org/index.php?topic=447878.0

[24] This modeling assumption that only a fraction of players can actively re-adjust their decisions, in the same spirit of Calvo (1983), is widely used in the literature (e.g., Burdzy, Frankel, and Pauzner (2001) and He and Xiong (2012)).

[25] We discuss in an earlier draft the case where active miners are endowed with fixed hash rates, which does not change our findings concerning the industrial organization of mining pools.

Taking the fee vector $\{f_m\}_{m=1}^M$ and passive hash rates $\{\Lambda_{pm}\}_{m=1}^M$ as given, these active miners can acquire and allocate hash rates to the above $m$ pools. Optimal allocation among existing pools, rather than a binary decision of participation or not, plays a key role in our analysis. In practice, some miners also recognize this benefit of allocating hash rates across many pools, even though no formal justifications are given.[26]

For an active miner facing $\{\Lambda_{pm}\}_{m=1}^M$ and $\{f_m\}_{m=1}^M$, the payout when allocating a hash rate of $\lambda_m$ to pool $m$ is

$$X_m = \frac{\lambda_m}{\Lambda_{am} + \Lambda_{pm}} \tilde{B}_m (1 - f_m) R, \tag{9}$$

where $\Lambda_{am}$ ($a$ stands for active mining) is the hash rate contribution to pool $m$ from all (symmetric) active miners. Recall that throughout the paper we use lower case $\lambda$ to indicate individual miner's decisions while upper case $\Lambda_m$ for hash rates at the pool level. Our continuum specification of miners implies that for each individual miner $\lambda_m$ is infinitesimal relative to the pool size $\Lambda_m$; this is why $\lambda_m$ does not show up in the denominator of Eq.(9). Finally, an infinitesimal miner with infinitesimal risk tolerance would not solo mine, as long as $f_m < 1$ for some $m$.[27]

As a result, the active miner chooses $\{\lambda_m\}_{m=1}^M$ to maximize

$$\mathbb{E}\left[u\left(\sum_{m=1}^M X_m - C\sum_{m=1}^M \lambda_m\right)\right] = \mathbb{E}\left[u\left(\sum_{m=1}^M \left(\frac{\lambda_m \tilde{B}_m (1-f_m)}{\Lambda_{am} + \Lambda_{pm}}\right) R - C\sum_{m=1}^M \lambda_m\right)\right],$$

where we have denoted $cT$ as $C$. Since our analysis works under any choice of $T$, for brevity of notation we further normalize $T/D = 1$. The certainty equivalent calculation based on exponential preference in Eq.(3) implies that the hash allocation to each pool decouples from one another, and the optimization is equivalent to

$$\max_{\lambda_m \geq 0} \left[\frac{\Lambda_{am} + \Lambda_{pm}}{\rho\Lambda}\left(1 - e^{-\frac{\rho R(1-f_m)\lambda_m}{\Lambda_{am}+\Lambda_{pm}}}\right) - C\lambda_m\right], \forall m, \tag{10}$$

[26] See forum discussions: "*Mining pools are used primarily to reduce variance, and the larger the pool, the more effective it is for this purpose. There is a simple way to decrease the variance further: Mine in multiple pools.*"

[27] Formally, each miner with $\Sigma\lambda_m \cdot di$ hash rates has a risk tolerance of $\frac{1}{\rho} \cdot di$ (or, an absolute risk aversion of $\frac{\rho}{di}$, where $di$ is the measure of an infinitesimal miner so that $\int di = N$ (as a result, the aggregate risk tolerance of miners is $\frac{N}{\rho}$). The certainty equivalent of solo mine of an infinitesimal miner, which is given in Eq.(4), can be shown to be of a lower order than Eq.(10).

where the global hash rate $\Lambda$ is

$$\Lambda = \sum_{m=1}^{M} (\Lambda_{am} + \Lambda_{pm}). \tag{11}$$

In each miner's objective (10), the global hash rate $\Lambda$ scales down the winning probability of each participating hash rate, so that in aggregate the block generation process is kept at a constant. This is a feature of many proof-of-work-based blockchain protocols such as Bitcoin, and the negative externality is important for understanding our results later.

In our setup, we have implicitly assumed that the infinitesimal active miners lack the expertise to become pool managers (they remain customers of mining pools). This is consistent with the following two facts: first, most miners simply run lightweight nodes (instead of running full nodes); and second, setting up and maintaining a mining pool is an elaborate process beyond most miners' sophistication.

## 3.2 Definition of Equilibrium

We focus on a class of symmetric subgame perfect equilibria in which homogeneous active miners take identical strategies. The notion of "subgame" comes from active miners reacting to the fees posted by the $M$ pools. In other words, all (homogeneous) active miners take symmetric best responses to any (on- and off-equilibrium) fees, and each pool faces an aggregate demand function (of the fee vector).

**Definition.** *A symmetric subgame perfect equilibrium in which homogeneous players take identical strategies is a collection of* $\{f_m\}_{m=1}^M$ *and* $\{\lambda_m\}_{m=1}^M$ *so that*

*(1)* ***Optimal fees:*** $\forall m \in \{1, 2, \cdots, M\}$, $f_m$ *solves pool manager* $m$*'s problem in (8), given* $\{f_{-m}\}$ *set by other pool managers;*

*(2)* ***Optimal hash rates allocations:*** *Given* $\{f_m\}_{m=1}^M$ *and* $\{\Lambda_m\}_{m=1}^M$, $\{\lambda_m\}_{m=1}^M$ *solve every active miner's problem in (10);*

*(3)* ***Market clearing:*** $N\lambda_m = \Lambda_{am}$.

## 3.3 A Frictionless Benchmark

The initial size distribution of mining pools is directly captured by passive hash rates $\{\Lambda_{pm}\}_{m=1}^M$ in our model. To highlight the role of passive hash rates in our model, we first

analyze a frictionless benchmark without passive mining.

**Proposition 2** (Irrelevance of Pool Size Distribution)**.** *Suppose* $\forall m \in \{1, 2, ..., M\}$, $\Lambda_{pm} = 0$. *The following allocation constitutes a unique class of symmetric equilibira:*

*(1) Pool managers all charge zero fees:* $f_m = 0$ *for all* $m \in \{1, 2, ..., M\}$*;*

*(2) Active miners choose any allocation* $\{\lambda_m\}_{m=1}^M$ *so that the global hash rates* $\Lambda$ *satisfies*

$$\Lambda = N \sum_{m=1}^{M} \lambda_m = \frac{R}{C} e^{-\rho R/N}. \tag{12}$$

*In this class of equilibra, every active miner owns an equal share of each mining pool, and the exact pool size distribution* $\{\Lambda_{pm}\}_{m=1}^M$ *is irrelevant.*

Proposition 2 shows a stark irrelevance result of pool size distribution for the purpose of risk sharing. In this class of equilibria, the global hash rate that miners acquire is $\Lambda = \frac{R}{C} e^{-\rho R/N}$, so that for each miner the marginal benefit of acquiring additional hash rate hits the constant acquisition cost $C$. Under zero fees, each individual miner maximizes his objective in (10). Fixing the total hash rate $\Lambda$ in this economy, the allocation among pools reaches full risk sharing among all miners.[28] Pool managers charge zero fees due to Bertrand competition, otherwise one pool manager can cut her fee to steal the entire market, thanks to the identical services the pools provide without passive hash rates.

**Fallacy of risk sharing and pools.** Numerous discussions in the blockchain community have focused on the centralization implications of mining pools, i.e., the better risk sharing provided by larger pools would attract even more hash rates and lead to further concentration. Proposition 2 rejects this fallacy based on a Modigliani-Miller insight: In a frictionless market, investors can perfectly diversify on their own, nullifying the risk sharing rationale for conglomerates. In other words, as long as miners can join pools in a frictionless way, one should not expect a single large pool to emerge.

In practice, reallocating between pools involves simply changing one parameter in the mining script and hence participating in multiple pools entails negligible transaction cost.[29]

[28] An alternative way to obtain full risk sharing is through "insurance" contracts with pure financial transfers. Such contracts could in theory allow each miner to solve their individual problems and therefore getting rid of the over-concentration concern. Such contracts are however difficult to implement in reality, due to costly-to-observe hash rates, and are rarely used. Another alternative is P2P pools, which require all participating miners to run full nodes. They constitute a negligible market share.

[29] There is a key difference between Bitcoin mining pools and traditional firms that provide valuable

As a result, joining $m$ pools with proper weights, so that each miner owns equal share of each pool, is equivalent to joining a single large pool with the aggregate size of these $m$ pools. Precisely because individuals can allocate their hash rates to diversify by themselves, forming large pools is unnecessary for risk-sharing purposes.

Given that miners in practice increasingly recognize the diversification benefits of mining in multiple pools, our theoretical insight has practical relevance in that over-concentration should not be a concern absent other frictions.[30] We show later that even though the key friction $\Lambda_{pm} > 0$ give market power to pools, the natural forces in the resulting monopolistic competition also counteract over-concentration.

**Pool collusion?** Potential collusion among a subset of pool managers do not change the result. In the benchmark setting, competition between two parties (potentially colluding groups) would drive the equilibrium fee to zero and render the distribution of pool size irrelevant. Even if all incumbent managers collude, new entrants (once we allow them in Section 6.1) would present similar competitive force. Collusion only matters when we introduce the passive mining friction $\Lambda_{pm}$. Still, to the extent that pool managers share the benefits from collusion, we can simply view colluding pools as one pool with a larger $\Lambda_{pm}$.

# 4 Equilibrium Characterization and Implications

We now allow the passive mining friction $\Lambda_{pm} > 0$, and characterize the equilibrium quantity and distribution of mining activities. $\Lambda_{pm}$ introduces heterogeneity across pools, pins down the equilibrium pool-size distribution, and reveals how mining pools affect the arms race in a realistic setting with market powers. We impose a simple parametric assumption.

insurance to workers against their human capital risks (e.g., Harris and Holmstrom (1982); Berk, Stanton, and Zechner (2010)): In the Bitcoin mining industry, it is easy for miners to allocate their computational power across multiple pools, just like in standard portfolio allocation problems in financial investment. In contrast, it is much harder for workers to hold multiple jobs.

[30] Our insight is also shared by some practitioners, though no formal argument or analysis has been put forth. For example, an interesting forum post remarks that mining in multiple pools "*not only helps variance for individual miners, but is healthier for the network. In the current standard usage, there is a 'the rich get richer, the poor get poorer' tendency where larger pools are more attractive and thus grow even larger, and all else being equal, the equilibrium is a single huge pool (thankfully, all else is not equal). If miners adopt the proposed strategy, the tendency will be to maintain the status quo distribution, so pools can rise and fall based on their merits. Miners will enjoy the low variance of a single huge pool, without the centralization of power problem.*"

**Assumption 1.** $\rho R < N$.

In our model, the aggregate risk tolerance of a measure $N$ of CARA active miners is $\frac{N}{\rho}$. Assumption 1 essentially requires that the implied CRRA risk aversion, which is $W\frac{\rho}{N}$ with $W$ being the aggregate wealth of Bitcoin community, to be below $\frac{W}{R}$, with $R$ being the dollar reward of each block. This trivially holds for reasonable CRRA coefficients (e.g., 2.)

## 4.1 Active Miners' Hash Rates Allocations

Since each infinitesimal individual active miner within the continuum takes the fee vector $f_m$, and more importantly the pool $m$'s total hash rates $\Lambda_m = \Lambda_{am} + \Lambda_{pm}$ as given, the first order condition from miners' maximization (10) gives,

$$\underbrace{\frac{R(1-f_m)}{\Lambda}}_{\text{risk-neutral valuation}} \underbrace{e^{-\rho R(1-f_m)\frac{\lambda_m}{\Lambda_{am}+\Lambda_{pm}}}}_{\text{risk aversion discount}} = \underbrace{C}_{\text{marginal cost}} . \tag{13}$$

The left (right) hand side gives the marginal benefit (cost) of allocating $\lambda_m$ to a pool with size $\Lambda_m = \Lambda_{am} + \Lambda_{pm}$, wherein the first term is the risk-neutral valuation of the marginal benefit to hash rate: reward times the probability of winning ($\frac{1}{\Lambda}$), adjusted by proportional fee. The second term captures the miner's risk-aversion discount. Fixing allocation $\lambda_m$, the larger the pool size $\Lambda_m$ he participates, the smaller the discount — as illustrated in Section 2.3; Fixing the pool size, the risk-aversion discount however worsens with his allocation $\lambda_m$. Since the optimal allocation rule equates marginal benefit with marginal cost, the better risk-sharing benefit from a larger pool leads to a higher active hash rate allocation.

In equilibrium we have $\Lambda_{am} = N\lambda_m$, therefore

$$\frac{\lambda_m}{\Lambda_{pm}} = \max\left\{0, \frac{\ln\frac{R(1-f_m)}{C\Lambda}}{\rho R(1-f_m) - N\ln\frac{R(1-f_m)}{C\Lambda}}\right\}, \tag{14}$$

where zero captures the corner solution of a pool not attracting any active miners (e.g., when $f_m$ is high enough). Equation (14) leads to the following proposition that relates pool fees to the equilibrium active hash-rate allocation in each pool.

**Proposition 3** (Active Mining Allocation)**.** *In any equilibrium, and for any two pools $m$ and $m'$,*

1. *If* $f_m = f_{m'}$ *, then* $\frac{\lambda_m}{\Lambda_m} = \frac{\lambda_{m'}}{\Lambda_{m'}}$*;*

2. *If* $f_m > f_{m'}$ *then we have* $\frac{\lambda_m}{\Lambda_m} \leq \frac{\lambda_{m'}}{\Lambda_{m'}}$*. If in addition* $\lambda_{m'} > 0$*, then* $\frac{\lambda_m}{\Lambda_m} < \frac{\lambda_{m'}}{\Lambda_{m'}}$*.*

Proposition 3 tells that pools that charge the same fee grows at the same proportion, and pools that charge higher fees grow slower.

## 4.2 Pool Managers' Fee-setting

For pool owners, the objective in (8) can be written as

$$\frac{\Lambda_{am}(f_m) + \Lambda_{pm}}{\Lambda(f_m, f_{-m})} \left(1 - e^{-\rho R f_m}\right) = \frac{\Lambda_{am}(f_m) + \Lambda_{pm}}{\Lambda_{am}(f_m) + \Lambda_{pm} + \Lambda_{-m}} \left(1 - e^{-\rho R f_m}\right) \tag{15}$$

where $\Lambda_{-m} = \sum_{m' \neq m} (\Lambda_{am'} + \Lambda_{pm'})$ is the global hash rate minus pool $m$'s. Compared to the miner's problem in (10), pool owners engage in a monopolistic competition, and take into consideration that $f_m$ not only affects their own pools' hash rates but also the global hash rate. Plugging Eq. (14) into Eq. (15) gives

$$\underbrace{\frac{1 - e^{-\rho R f_m}}{\Lambda(f_m)} \cdot \max\left\{1, \frac{\rho R(1 - f_m)}{\rho R(1 - f_m) - N \ln \frac{R(1-f_m)}{C\Lambda(f_m)}}\right\}}_{\text{value per unit of initial size } \Lambda_{pm}} \cdot \underbrace{\Lambda_{pm}}_{\text{initial size}} \tag{16}$$

Eq.(16) illustrates the dependence of global hash rate on pool fees: when each pool manager sets the fee to maximize her value per unit of initial size $\Lambda_{pm}$, she also takes into account the impact of her fee on the global hash rates $\Lambda(f_m)$.

Proposition 4 characterizes a monotonicity property between a pool's passive hash rate and the optimal fee it charges in equilibrium.

**Proposition 4** (Endogenous Pool Fees)**.** $\forall m, n \in \{1, \cdots, N\}$ *where* $\Lambda_{am} > 0$ *and* $\Lambda_{an} > 0$*,* $\Lambda_{pm} > \Lambda_{pn}$ *implies* $f_m^* > f_n^*$*. In other words, among pools that grow, a larger pool charges a higher fee.*

Note that if a pool charges $f_m = 1$, it would not attract active miners and grow. Therefore a growing pool must be charging an interior fee less than one. The intuition for Proposition 4 is rooted in that pools with more initial passive hash rates take into account their larger

"global hash rate impacts." To see this, suppose pool owners ignore the fee impact on global hash rate and view $\Lambda(f_m)$ as a constant, then the optimal choice of $f_m$ should maximize the term "value per unit of $\Lambda_{pm}$", which is independent of $\Lambda_{pm}$, leading to all managers charging the same fee. However, pool managers who behave as oligopolists understand that $\Lambda'(f_m) < 0$; they take into account the fact that charging a lower fee brings more active miners, pushing up the global hash rates $\Lambda$ and hurting her pool's profit. In the extreme, a monopolist pool manager fully internalizes the cost of higher global hash rates. Because every unit of active hash rate affects the aggregate hash rates equally, on the margin, a larger pool who takes into account her "global hash rate impact" has a stronger incentive to raise fees and curb the increase in mining difficulty, just like firms with larger market power charge higher prices and produce less in a standard oligopolistic competition.[31]

We next discuss two implications of the equilibrium: (i) mining pools as a financial innovation escalates the mining arms race (Section 4.3), and (ii) there is a mean-reverting force in pool growth (Section 4.4).

## 4.3 Financial Innovation and Arms Race

Recall that absent mining pools, there is no solo-mining — an artifact of our modeling choice of the continuum of infinitesimal miners (see footnote 27). To find an estimate of solo-mining similar to that in a model with $N$ discrete active miners, and to compare mining activities with and without mining pools in an empirically relevant manner, we define solo-mining as active miners acting in groups of unit measures, and then apply the optimality condition (13) so that no active miner would like to acquire more hash rates. Then the total global hash rate under solo mining only is $\frac{R}{C}e^{-\rho R}$, which is significantly smaller than the total global hash rate with full risk sharing, $\frac{R}{C}e^{-\rho R/N}$, especially for large $N$.

Our model is an example of financial innovation/vehicle that seemingly benefits individual miners but in aggregate could lower their welfare (which in the model is the opposite of global hash rates). Miners' welfare losses become significant precisely when the risk-sharing benefit of mining pools is large — say, when the risk-aversion $\rho$ is high, or the measure of active miners $N$ is large. We caution the readers that our simple setup does not account for benefits of using blockchains such as online security. The actual socially optimal mining

[31] This result is not driven by that pool managers benefit from charging a higher fee to get higher revenues from the passive miners. In fact, absent active mining and the "global hash rate impact," all pools would charge the same fee $f = 1$ to maximize the revenue from passive miners.

has to be positive in reality. Had we modeled the benefit of mining, it is possible that if risk aversion were sufficiently high then the risk-sharing innovation from mining pools could promote efficient levels of mining under certain parameter ranges.[32] Our modeling choice is motivated by the goal to illustrate in a simple and transparent way the economic forces of risk-sharing and monopolistic competition, which are important in the crypto-mining industry. Considering the benefits of mining would not change our theoretical insights here. Moreover, at least for Bitcoin, it is hard to justify that its usage value exceeds the cost of energy consumption at the present.

This economic force, which is already transparent even in the frictionless benchmark, is of first-order importance for PoW-based blockchain consensus generation. The equilibrium global hash rates are lower in the main model with frictions, because active miners face positive fees that discourage their hash rate acquisition. However, under reasonable parameter choices, the implied global hash rates with mining pools can still multiply that without mining pools.

For illustration, it suffices to study the case with pools of homogeneous size, and compare the resulting endogenous global hash rates to the solo-mining case as well as the frictionless benchmark. Say $\Lambda_{pm} = \Lambda_p$ for all $m \in \{1, ..., M\}$, and focus on the situation where fees take interior solutions. After some simplifications of the first-order conditions of (8) and (10), one can show that the endogenous fee $f^*$ (charged by all pools) solves $\rho R\left(1-f\right)\left(1-z\left(f\right)\right) = N \ln \frac{R(1-f)z(f)}{MC\Lambda_p}$, and the global hash rates $\Lambda = \frac{M\Lambda_p}{z(f^*)}$, with $z\left(f\right) \equiv \frac{(M-1)\left(1-e^{-\rho Rf}\right)[N-\rho R(1-f)]}{Me^{-\rho Rf}\rho^2R^2(1-f)-(M-1)\left(1-e^{-\rho Rf}\right)}$.

Figure 2 provides a quantitative illustration. Each panel in Figure 2 plots the endogenous global hash rates, as a function of reward $R$, under three scenarios: (i) solo-mining without pools; (ii) full risk-sharing implied by Proposition 2 without passive mining friction; and (iii) monopolistic competition with passive hash rates as initial pool size, with $M = 2$. Panels A and B plot the global hash rates $\Lambda$ for two risk-aversion coefficients $\rho$; Panels C and D plot $\Lambda$ for two values of the active miner measure $N$.

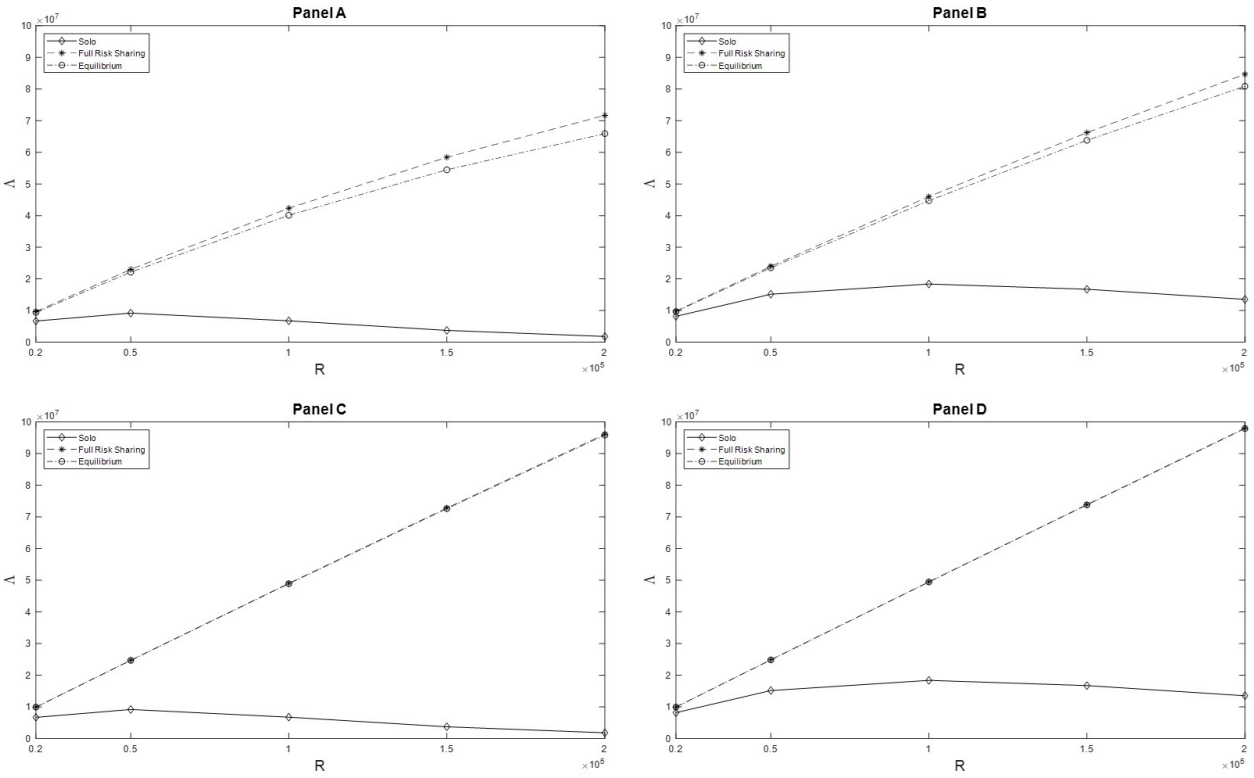
First, we observe that for solo-mining, the implied global hash rates increases with reward $R$ initially but decreases when $R$ is sufficiently large; this is because the risk becomes overwhelming when $R$ increases.[33] Second, when we compare Panel A (B) with C (D) which feature $N = 10$ and $N = 100$ respectively, they by definition have the same solo-

[32] We thank an anonymous referee for encouraging us to clarify the model's implications on social welfare.
[33] A result of CARA preference which has no wealth effect; the risk increases with $R$.

mining outcomes, but their full risk-sharing hash rates differ by at most a factor of 1.4. The relative small factor is expected from standard portfolio theory: quantitatively further risk-diversification provides little benefit when an individual is already diversified across about 20 assets (pools, in our setting; see Figure 7.10 on page 254 in Fama, 1976).

Figure 2: **Global Hash rates under Solo, Full Risk Sharing, and Equilibrium**

Global hash rates $\Lambda$ is plotted against block reward $R$ under various parameters. We consider symmetric $M$ pools each with passive hash rates $\Lambda_p = 3 \times 10^6$. The common parameter is $C = 0.002$, and other parameters are given as following. Panel A: $M = 2, N = 10, \rho = 2 \times 10^{-5}$; Panel B: $M = 2, N = 10, \rho = 1 \times 10^{-5}$; Panel C: $M = 2, N = 100, \rho = 2 \times 10^{-5}$; Panel D: $M = 2, N = 100, \rho = 1 \times 10^{-5}$.




Now we move on to the equilibrium outcome under mining pools with passive hash rates. Relative to solo mining, both the full risk-sharing and the mining-pool equilibrium produce about five times of global hash rates for $\rho = 2 \times 10^{-5}$ and $R = 10^5$, for both levels of $N$. This wedge gets amplified greatly for $R = 2 \times 10^5$, which is reasonable for peak Bitcoin price in December 2017: the hash rates with mining pools rise to about ten times of that with only solo mining. The arms race escalates when miners are more risk-averse.

As expected, the homogeneous two-pool equilibrium generates lower global hash rates compared to the full risk-sharing equilibrium. Intuitively, pool managers with some market power take into account the arms race effect and hence discourage active miners' hash rate

acquisition by raising their fees. Even when we give the best chance of this market-power force to produce a countervailing effect by considering the lowest possible of number of pools (here, $M = 2$), quantitatively there is no big difference from the full risk-sharing case. In fact, the difference between the full risk-sharing and two-pool cases becomes invisible when $N$ is large (Panel C and D). Intuitively, when there are more competing active miners (i.e. $N$ is large), pools engage in a more aggressively competition which is the root of arms race.

The take-away from Figure 2 is that no matter whether we consider the friction of passive mining, the emergence of mining pools as a form of financial innovation escalates the mining arms race and contributes to its explosive growth in energy consumption in recent years. In fact, one can show that with mining pools the aggregate hash power is always higher than without mining pools, as long as those mining pools attract positive hash rate in equilibrium.[34]

Even though in the data, both the growing dominance of pooled mining and the increase in hash rates are correlated with the rising price of Bitcoin, we underscore that for any given price level, mining pools significantly amplifies the global hash rates once we consider risk aversion of miners.

## 4.4 Equilibrium Pool Growth

Propositions (3) and (4) lead to a key conclusion about the distribution of pool sizes.

**Corollary 1** (Pool Growth Rate)**.** *A pool with a larger initial size $\Lambda_{pm}$ has a (weakly) lower growth rate $\frac{\Lambda_{am}}{\Lambda_{pm}}$.*

This result implies that profit-maximizing mining pools do not create excessive centralization, because a natural force from the market power of larger pools combined with the arms race nature of the mining technology limits their growth.

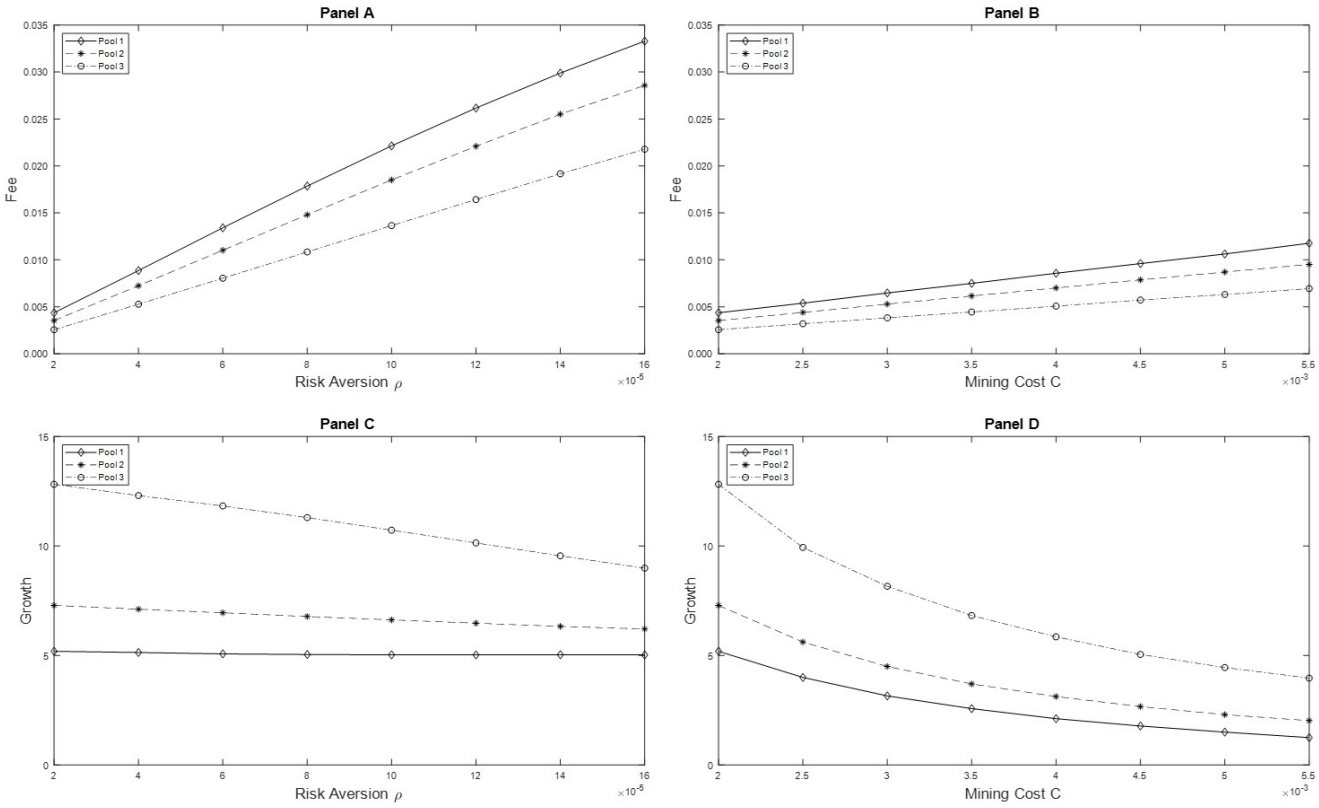
For illustration, Figure 3 studies a three-pool equilibrium with comparative statics for the endogenous fees charged by pool managers $\{f_1, f_2, f_3\}$ as well as equilibrium pool net growth $\{\Lambda_{a1}/\Lambda_{p1}, \Lambda_{a2}/\Lambda_{p2}, \Lambda_{a3}/\Lambda_{p3}\}$. Without loss of generality, we assume $\Lambda_{p1} > \Lambda_{p2} > \Lambda_{p3}$.

[34] To see this, suppose the contrary that in equilibrium the aggregate hash power is less than an equilibrium with only solo-mining, then it means $e^{-\rho R}$ (aggregate hash mining solo as discussed in Section 4.3) is greater than $(1 - f_m)e^{-\rho R(1-f_m)/N}$ (aggregate hash with mining pools for any pool m with positive active mining) for any pool m with non-trivial active hash. However, for someone to not move some active hash from pool m to solo-mining, the opposite has to hold according to the marginal benefit of allocating hash rate as derived in Equation (20) in the Appendix, which gives a contradiction.

Panel A presents how the equilibrium fees respond to exogenous changes in the risk aversion $\rho$ of this economy, and Panel B presents how the equilibrium fees vary with the unit hash rate acquisition cost $C$. Not surprisingly, when risk aversion increases, individual miners' demands for risk sharing increase, and mining pools charge higher fees as shown in Panel A of Figure 3. At the same time, larger pools charge higher fees, as predicted by Proposition 4. Panel C shows that larger pools hence grows slower.

Figure 3: **Comparative Statics of Pool Fees and Growth**

Equilibrium fees $\{f_1, f_2, f_3\}$ and the net pool growth rates $\Lambda_{a1}/\Lambda_{p1}, \Lambda_{a2}/\Lambda_{p2}$, and $\Lambda_{a3}/\Lambda_{p3}$ are plotted against miner risk aversion $\rho$ and unit hash rate cost $C$, respectively. The baseline parameters are: $R = 1 \times 10^5$, $\Lambda_{p1} = 3 \times 10^6, \Lambda_{p2} = 2 \times 10^6$, $\Lambda_{p3} = 1 \times 10^6$, and $N = 100$. In Panel A and C: $C = 0.002$. In Panel B and D: $\rho = 2 \times 10^{-5}$.




Panel B and D illustrate how the equilibrium outcomes change when we vary the constant hash rate acquisition cost $C$. As the hash rate acquisition cost $C$ lowers, more active hash rates enter, and pool managers have stronger incentives to lower fees to compete for them. Fees and pool growths across pools are similar to other panels.

Importantly, this absence of dominant pools over time implies that the market power and internalization of mining externality by pool owners (discussed in Section 4.3) is small relative

to the extent risk sharing through mining pools encourage individuals to acquire additional hash rate. Consequently, even though Figure 2 depicts homogeneous pools, the aggravation of the mining arms race would not be mitigated much in the presence of heterogeneous pools.

We also remind the readers that our theoretical findings, especially Propositions 3 and 4 and Corollary 1 are not qualitatively dependent on the particular parametrization we use for plotting the illustration figures.

# 5 Empirical Evidence

Our theoretical analyses so far offer three predictions. First, global hash rates grow significant as mining pools increasingly dominate the Bitcoin mining industry, as illustrated in Figure 1. This section provides supporting evidence for the other two cross-sectional predictions, that a pool with a larger initial size tends to (i) charge a higher fee, and (ii) grow slower in percentage terms.

**Linking model to data.** To be exact, our model predicts that pools with larger passive mining charge higher fees (Proposition 4) and attracts less active mining as a percentage of their passive mining (Corollary 1). To relate this to pool size empirical with a panel data, we have assumed that the pool size (or a fixed fraction of it) from a previous period is equivalent to the initial passive hash of the current period.

To justify this assumption, one convenient way to think about passive hash rate is that in every period there are naive agents who are unsophisticated or inattentive, and therefore simply allocate their hash power in proportion to the saliency of pools (or only to the best-known pool), which (or whose probability) is proportional to the size of the pool in the previous period because larger pools have better websites and greater publicity. Another way to interpret passive hash rate is that a fixed fraction of all miners from the previous period are randomly chosen across various pools to be inattentive and simplify keep their hash allocations as in the previous period. Yet another possibility is that a fixed fraction of all miners in a pool from the previous period becomes loyal supporters because of their experience for other services the pool provides or behavioral biases (affirmation bias, for example, would lead a miner to continue allocating the hash rate to the pool she has been allocating to earlier, to justify the previous action is correct.) These would also give an initial hash rate proportional to the previous periods pool size for each pool.

In reality, a larger pool might have greater publicity (e.g., through forum discussions and google search) and attract more nave miners, but it is unlikely that it has constant return to scale to attract proportionally more naive miners, because after all, searching for available pools and learning about them are not too costly in this digital age. What is more realistic would be naive agents almost randomly chance upon various pools, so larger pools do get more of them, but not necessarily proportionally more. Our empirical tests can accommodate such cases in which a previously larger pool attracts, when going into the next period, greater passive mining (be them inattentive, native miners or loyal supporters/partners), but not disproportionally greater.

**Data description.** Our data consist of two major parts, one on pool size evolution and the other on pool fee/reward type evolution. In the first part, a pool's size (share of hash rates) is estimated from block-relay information recorded on the public blockchain (see BTC.com). Specifically, we count the number of blocks mined by a particular pool over some time interval, to be divided by the total number of newly mined blocks globally over the same time interval; the ratio is the pool's estimated hash rate share. Balancing the trade-off between estimation precision and real-timeness, we take the time interval to be weekly.[35] In the second part, information about fee contracts is obtained from Bitcoin Wiki. We scrape the entire revision history of the website (477 revisions in total) and construct a panel of pool fee evolutions over time.[36] Pool fees are aggregated to quarterly frequency by simple average. The two parts are then merged to construct a comprehensive panel on pool size and fee evolution. Table 1 in Section 2 has provided summary statistics of the data. Our main analysis is at a quarterly frequency given potentially lagged adjustments.

**Empirical results.** Every quarter we first sort pools into deciles based on the start-of-quarter pool size (estimated hash-rate share within the first week). We then calculate the

[35]Our estimation procedure is standard. For example, blockchain.info provides real-time updates about estimated hash rate distribution over the past 24 hours, 48 hours, and 4 days using the same method. Bitcoinity tracks about 15 large mining pools' real time hash-rate changes on an hourly basis. We favor weekly frequency over daily frequency because among all the pools that successfully find at least one block within a quarter, only (more than) 1.96% (42%) do not find any blocks within the first week (day) of that quarter. This is important because later analysis uses the estimated hash-rate share within the first week as the initial pool size for the quarter.

[36]Two large pools are missing from the Wiki: Bixin (which was available in the wiki as HaoBTC prior to Dec 2016), and BTC.top, for which we fill their information through direct communication with the pools. Bitfury, which is also missing from the Wiki, is dropped as it is a private pool not applicable to our analysis.

average proportional fee and average log growth rate across mining pools for each decile.

Figure 4: **Empirical Relationships of Pool Sizes, Fees, and Growths**

This figure shows the binned plots of the changes in *logShare* (Panel A) and *Proportional Fees* (Panel B) against *logShare*. Share is the quarterly beginning (the first week) hash rate over total market hash rate. Fees are the quarterly averaged proportional fees. Within each quarter $t$, $\Delta logShare_{i,t+1}$, Proportional $\text{Fee}_{i,t}$, and $logShare_{i,t}$ are averaged within each $logShare_{i,t}$ decile, and these mean values are plotted for 2012-2013, 2014-2015, and 2016-2017, respectively. Red lines are the fitted OLS lines, with t-stat reported at the bottom. Data sources and descriptions are given in Section 5.

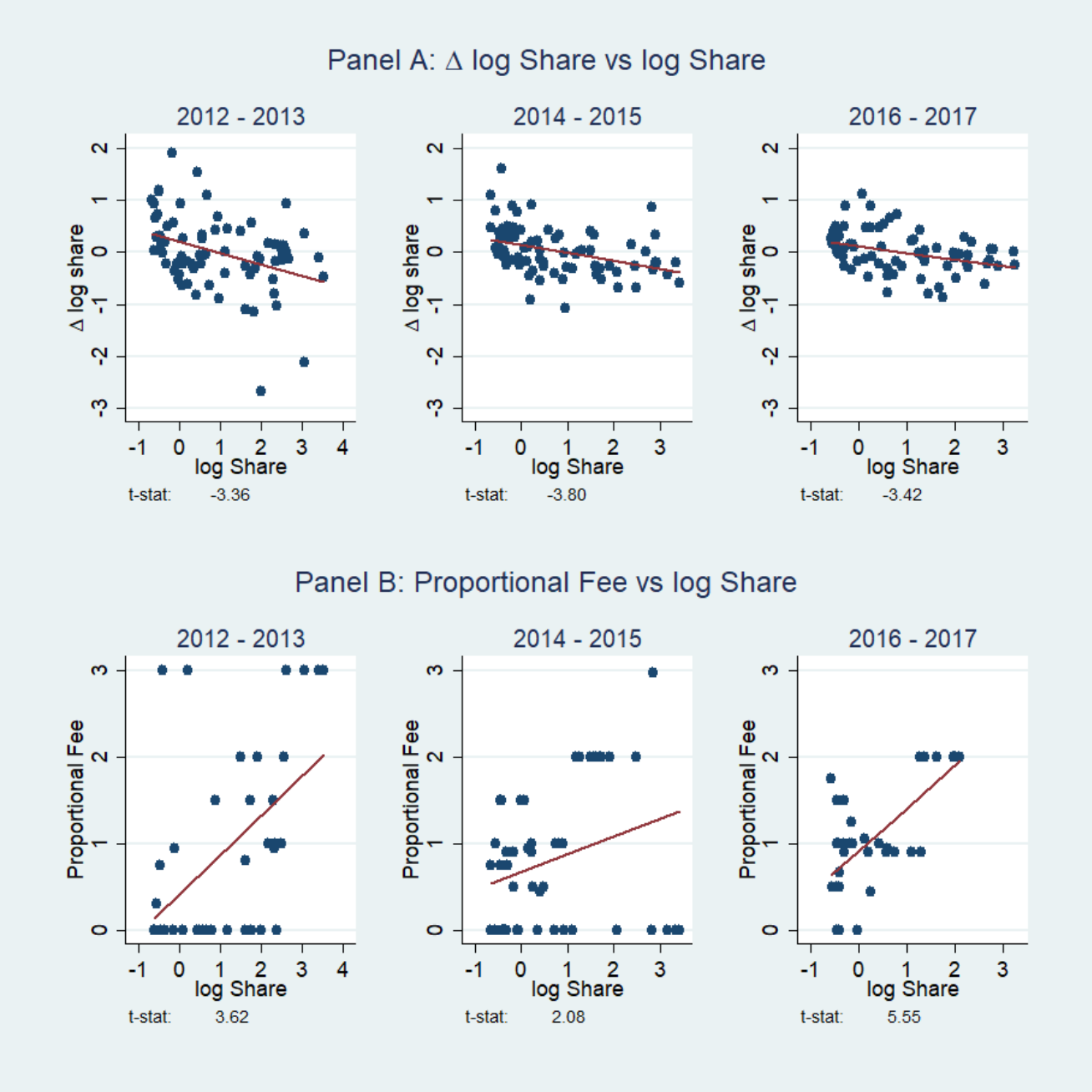


Table 2: **Pool Sizes, Fees, and Growths: Regression Results**

This table reports the regression results when we regress *Proportional Fee* and $\Delta logShare$ on *logShare*, respectively. Share is the quarterly initial hash rate over total market hash rate. Fees are the quarterly averaged reward fees. Within each quarter t, $\Delta logShare_{i,t+1}$, *Proportional* $Fee_{i,t}$, and $logShare_{i,t}$ are averaged within each $logShare_{i,t}$ decile. The resulting mean values of $\Delta logShare_{i,t+1}$ and *Proportional* $Fee_{i,t}$ are then regressed on the mean value of $logShare_{i,t}$ respectively over two years in the left three columns, over the entire sample period in the fourth column, and in addition control for quarter fixed effects in the fifth. Data sources and their descriptions are given in Section 5.

| | Panel A: $\Delta logShare$ | | | | |
|---|---|---|---|---|---|
| | 2012-2013 | 2014-2015 | 2016-2017 | 2012-2017 | 2012-2017 |
| *logShare* | -0.219** | -0.153*** | -0.122** | -0.176*** | -0.176*** |
| | (-3.36) | (-3.80) | (-3.42) | (-6.12) | (-6.00) |
| Intercept | 0.200* | 0.135* | 0.108* | 0.153*** | |
| | (2.01) | (2.47) | (2.21) | (3.77) | |
| Quarter FE | No | No | No | No | Yes |
| Nobs | 73 | 80 | 78 | 235 | 235 |
| | Panel B: *Proportional Fee* | | | | |
| | 2012-2013 | 2014-2015 | 2016-2017 | 2012-2017 | 2012-2017 |
| *logShare* | 0.452*** | 0.203* | 0.487*** | 0.318*** | 0.355*** |
| | (3.62) | (2.08) | (5.55) | (5.24) | (5.59) |
| Intercept | 0.431* | 0.683*** | 0.924*** | 0.700*** | |
| | (2.07) | (5.24) | (11.38) | (8.55) | |
| Quarter FE | No | No | No | No | Yes |
| Nobs | 38 | 51 | 37 | 126 | 126 |

$t$ statistics in parentheses
$* : p < 0.05, ** : p < 0.01, *** : p < 0.001$

Figure 4 shows scatter plots for these decile-quarter observations: Panel A (B) presents the relationship between initial pool size and proportional fee (subsequent pool size growth rate). For robustness, we present the scatter plots for three two-year spans 2012-2013, 2014-2015, and 2016-2017. As predicted by our theory, Panel A shows that larger pool grows in a slower pace, and Panel B shows that cross-sectionally a larger pool charges a higher fee. All regression coefficients are statistically significant at 5% level for all three time periods. Detailed regression results are reported in Table 2.

Before we move on to the next section, we would like to highlight that the above empirical patterns in the Cryptocurrency mining industry—i.e., a positive size-fee relation and a negative size-growth relation—should not be taken granted. For instance, in the passive asset management industry which basically offers index funds to retail investors, a larger fund actually charges lower fees; Hortaçsu and Syverson (2004) provide a search-based mechanism

to explain this empirical regularity. Moreover, although earlier studies on the size-growth relation indeed document that larger firms grow less (Caves, 1998; Rossi-Hansberg and Wright, 2007), the recent literature on ''superstar" firms finds increasing concentrations across various industries and hence a positive size-growth relationship in the past decades (Autor, Dorn, Katz, Patterson, and Van Reenen, 2017; Andrews, Criscuolo, Gal, et al., 2016). Our empirical results provide another data point on this important industry organization question.

# 6 Discussions and Extensions

In this section, we first examine how the market power of mining pools survives pool entry. We then discuss how our model applies to alternative consensus protocols such as proof-of-stake. Along the way, we also present an economist's perspective on several important issues such as the nature of risk and other centralization and decentralization forces.

## 6.1 Entry and Market Power of Mining Pools

Our model takes the pool managers with endowed passive hash rates as exogenously given. This section discusses the pool's intrinsic market power due to its passive hash rates, and show that our results are robust to potential entry of competing mining pools.

We first consider the possibility of free entry of pool managers without passive hash rates. In equilibrium, incumbents always charge strictly positive fees to some active miners. We then discuss the entry of pool managers with passive rates, so that the number of pools is endogenously determined by the entry condition.

**Pool entry without passive hash rates.** Denote the number of incumbent pools with passive hash rate by $M^I$. Suppose new pool managers can enter the market by incurring a setup cost $K \geq 0$ each; the case of $K = 0$ corresponds to the case of free entry. We assume that entrant pools do not have passive hash rates and start with $\Lambda_{pm} = 0$, $\forall m \in \{M^I + 1, \cdots, M^I + M^E\}$, where $M^E$ is the endogenous number of new entrants. Denote $M \equiv M^I + M^E$ the total number of (potential) mining pools.

We now show that without loss of generality, at most one pool without passive hash rates enters; and incumbent pools with $\Lambda_{pm} > 0$ always enjoy some market power.

**Proposition 5** (Entry and Market Power of Incumbent Pools)**.**

1. *For any $K > 0$, at most one pool enters. When $K = 0$, equilibrium outcomes for active miners' allocation and payoff are equivalent to the case with one pool entering and charging zero fee.*

2. *Incumbent pools with passive hash rates always charge positive fees and attract positive measure of active hash rate, even with free entry ($K = 0$).*

The first part of the proposition follows from Proposition 2. Entrant pools are homogeneous and compete away any net profit among themselves. Therefore in equilibrium at most one pool enters and breaks even. Proposition 2 implies that when $K = 0$, the size distribution of entry pools is irrelevant from active miners' perspective.

The second part has profound implications. Given that individual active miners face a portfolio diversification problem, incumbent pools always retain some monopolistic power even under free entry. For any fee $f_m$ charged by incumbent $m$, the marginal benefit of allocating the first infinitesimal hash rate to this incumbent can be calculated by setting $\lambda_m$ and $\Lambda_{am}$ to zero in $R(1-f_m)e^{-\rho R(1-f_m)\frac{\lambda_m}{\Lambda_{am}+\Lambda_{pm}}}$ in Eq. (13), which gives exactly the post-fee risk-neutral valuation,

$$\frac{R(1-f_m)}{\Lambda}. \tag{17}$$

Suppose, counter-factually, that an incumbent pool with positive passive hash rates charge zero fee $f_m = 0$; then the risk-neutral valuation $\frac{R}{\Lambda}$ in Eq. (17) must exceed the marginal cost $C$ in any equilibrium with strictly positive active mining (due to the risk-aversion discount in Eq.(13)).[37] As a result, incumbent pools start charging positive fees.

Compared with a standard perfectly competitive market wherein a Bertrand-type price competition allows entry firms to compete away any profit of incumbents, incumbent pools here with strictly positive passive hash rates face a monopolistic competition: They are essentially offering products with higher quality than entry pool with zero passive hash rates. In particular, the first infinitesimal unit of hash rates allocated in incumbent pools with $\Lambda_{pm} > 0$ corresponds to a risk-neutral valuation, while it has a strictly positive risk-aversion discount in the new entry pool without passive hash rates.

[37] In equilibrium, positive active mining in the entry pool with zero fee requires that $\frac{R}{\Lambda}e^{-\rho R/N} = C$, which implies that $\frac{R}{\Lambda} > C$.

We also note that with incumbents' market power, the active miners never achieve full risk sharing, resulting in a welfare distortion fixing the level of aggregate hash rates. But as we discussed earlier, the lack of full risk-sharing also alleviates the arms race and reduce energy consumption.

**Pool entry with passive hash rates.** Given that entrants without hash rates essentially offer inferior quality of goods, what if some new pool managers with passive hash rates can enter?

Note, for entry with passive hash rates, the entry costs are strictly positive ($K > 0$) including the acquisition cost of passive rates and set-up cost. Given a fixed set-up cost, a finite number of pools enter. Then the equilibrium outcome resembles the one in our main model, with an endogenous number of incumbent pools $M^I$ so that it is no longer profitable to enter. The nature of post-entry industrial organization of mining pools is qualitatively similar, with each pool exerting its monopolist power by charging positive fees to its active mining customers. As in any monopolistic competition, entry continues until the profits cannot cover the entry costs.

## 6.2 The Nature of Risk

Given that risk sharing drives the formation of mining pools, several issues regarding the nature of the risk are worth discussing. First, a miner's underlying mining risk $\tilde{B}$, i.e., whether and when a miner finds the solution, is idiosyncratic in its nature. Our paper emphasizes the importance of diversification, rather than pricing idiosyncratic risk (via pools). Idiosyncratic risk matters little for pricing exactly because agents diversify it away.

The idiosyncratic nature of mining risk may also lead to a hasty conclusion: risk-averse agents who are well-diversified on their financial wealth should be neutral to the idiosyncratic mining risk if they can engage in infinitesimal amount of mining. This claim is incorrect, because the celebrated asset pricing result holds only when agents can trade infinitesimal "shares" of assets with idiosyncratic risks (which, in a way, is similar to participating in mining pools). But in our model, without participating in pools, acquiring an infinitesimal amount of hash rate shrinks the probability of winning toward zero without changing the magnitude of (risky) reward.[38] If this reward is significant relative to the agent's con-

[38]In standard asset pricing models, an agent with utility function $u$ who consumes $\widetilde{C}$ and faces an asset

sumption/wealth, then risk-diversification benefits remain for this lottery with infinitesimal winning probability.

Second, there is anecdotal evidence that miners are under-diversified for their idiosyncratic mining incomes. It is also important to realize that throughout our observation period, the mining income often represents a significant source of the miner's total income, justifying the relevance of diversifying the idiosyncratic risk in this context.[39] Furthermore, as in the discussion of the now famous "fallacy of large numbers" by Samuelson (1963) and a further treatise by Ross (1999), mining over a long period of time does not help in general.

Third, why blockchain protocols randomize the allocation of newly minted cryptocurrencies or crypto-tokens to start with? Although outside our model, we believe the design is motivated by the need to ensure proper ex-post incentives of record-generation once a miner has mined a block. If a miner always gets paid deterministic rewards in proportion to his hash rate no matter who successfully mines the block, then a successful miner who puts in very little hash rate (and thus gets very little reward) worries less about not being endorsed by subsequent miners because the benefit of mis-recording could outweigh the expected cost of losing the mining reward.

Finally, we can easily introduce systematic risk in the mining reward $\tilde{R}$, which we take as deterministic so far. The Bitcoin mining reward these days is predominantly determined by the price of the Bitcoin. If—which is a big if—Bitcoin ever becomes an important private money that is free from inflation (due to rule-based supply), as some advocates envision, then its exchange rate against fiat money would presumably be driven by macroeconomic shocks such as inflation. It constitutes an interesting future study to analyze the role of systematic risk in our framework, especially when $\tilde{R}$ offers some diversification benefits for investors in the financial market.

---

with idiosyncratic payoff $\widetilde{R}$ and price $p$, solves $\max_\epsilon \mathbb{E}\left[u\left(\widetilde{C}+\epsilon\widetilde{R}-\epsilon p\right)\right]$. Then the Euler equation gives the risk-neutral pricing $p=\mathbb{E}[\widetilde{R}]$ if $\widetilde{R}$ is idiosyncratic. However, in our mining technology, the miner who can acquire infinitesimal hash rates solves $\max_\epsilon \epsilon\mathbb{E}\left[u\left(\widetilde{C}+R-\epsilon p\right)\right]+(1-\epsilon)\mathbb{E}\left[u\left(\widetilde{C}-\epsilon p\right)\right]$, as he receives $R$ with probability $\epsilon$. The curvature of $u$ enters in the valuation $p=\frac{\mathbb{E}[u(\widetilde{C}+R)-u(\widetilde{C})]}{\mathbb{E}\left[u'(\widetilde{C})\right]}$.

[39] The recent introduction of future contracts on CBOE and CME may alleviate this problem in a significant way, but it is unclear how long it takes for the miner community to actively trading on the future contracts or for more derivatives and insurance products to be introduced.

## 6.3 General Implications for Consensus Protocols

**Other proof-of-work blockchains** Our model can help us better understand the centralizing and decentralizing forces in other proof-of-work blockchains. For example, major cryptocurrencies such as Ethereum, Bitcoin Cash (BCH), Litecoin (LTC), and ZCash (ZEC), etc., all rely on PoW and share features captured in our model. They have all witnessed the rise of mining pools and similar trends in their mining industrial organizations.

**Proof-of-stake protocols** A popular alternative to the PoW protocol is the Proof-of-Stake (PoS) protocol. In PoS, independent nodes are randomly selected to append the blockchain, just like in PoW, but the probability to be selected is determined by the amount of "stake" held, instead of the amount of computing power consumed. Examples include Nxt and BlackCoin, where the calculation of "stake" involves the amount of crypto assets held (randomized block selection method), as well as Peercoin, where the calculation of "stake" involves how long a crypto asset has been held (coin age based system).[40]

Even though our model focuses on PoW protocols, its implications for the industrial organization of players in the decentralized consensus generation process applies to PoS equally well. This is because of PoS's similar features of risky rewards and negative externality. The same risk-sharing motive should drive the formation of "staking pools." This indeed happens: The largest players such as StakeUnited.com, simplePOSpool.com, and CryptoUnited typically charge a proportional fee of 3% to 5%. An individual's problem of allocating her stake is exactly the same as in (10), with $\lambda_m$ indicating the amount of stake allocated to pool $m$. All our results go through, except that in PoS the consensus generation process does not necessarily incur wasterful energy consumption.

Several recent trends in the blockchain universe are consistent with our model predictions: For example, in light of the high energy associated with PoW protocols, Ethereum plans to switch from PoW to PoS (known as Casper); Recognizing mining pools' inevitable rise, systems such as EOS adopts delegated-Proof-of-Stake (DPoS) in its consensus generation process, in which a small group of validators can take control of the network: DPoS stakeholders vote for delegates (typically referred to as block producers or witnesses) who maintain consensus records and share rewards with their supporting stakeholders, in propor-

[40] PoS systems are more environmentally friendly due to lower electricity consumption. While practitioners have criticized PoS systems citing a "nothing at stake" problem, Saleh (2017) shows that the problem goes away once we endogenize crypto-token price and the speed to consensus.

tion to their stakes after taking cuts, just like the pool managers in our model who charge fees and give out proportional rewards to individual miners.[41]

## 6.4 Centralization in Decentralized Systems

In this paper we focus on risk sharing and market power as a centralizing and decentralizing force. This perspective does not preclude other forces. For example, Chapman, Garratt, Hendry, McCormack, and McMahon (2017), de Vilaca Burgos, de Oliveira Filho, Suares, and de Almeida (2017), and Cong and He (2018) discuss how the concern for information distribution could make nodes in blockchain networks more concentrated.

The blockchain community has also proposed several reasons why a mining pool's size may be kept in check: (1) ideology: Bitcoin miners, at least in the early days, typically have strong crypto-anarchism background, for whom centralization is against their ideology. We think this force is unlikely to be first-order as Bitcoin develops into a hundred-billion-dollar industry; (2) sabotage: just like the single-point-of-failure problem in traditional centralized systems, large mining pools also attract sabotages, such as decentralized-denial-of-service (DDoS) attacks from peers.[42] While sabotage concerns could affect pool sizes, it is outside the scope of this paper; (3) trust crisis: it has been argued that Bitcoin's value builds on it being a decentralized system. Over-centralization by any single pool may lead to collapse in Bitcoin's value, which is not in the interest of the pool in question. Empirical evidence for this argument, however, is scarce. We find no significant correlation between the HHI of the mining industry with bitcoin prices. Nor do we find any price response to concerns about GHash.IO 51% attack around July in 2014.

Specifically in regards to our empirical findings, we also do not rule out other potential explanations. For example, higher prices for larger pools could easily be attributed to product differentiation or larger pools being more trustworthy. The growth of mining pools as mining increases could also simply be the natural maturing of the industry. However, we argue that

[41] Delegates on LISK, for example, offer up to more than 90% shares of the rewards to the voters. As of Oct 2018, about 80 percent offer at least 25% shares (https://earnlisk.com/). Some DPoS-based systems such as BTS and EOS traditionally have delegates paying little or no rewards to stakeholders, but that is changing. See, for example, https://eosuk.io/2018/08/03/dan-larimer-proposes-new-eos-rex-stake-reward-tokens/.

[42] See, for example, Vasek, Thornton, and Moore (2014). Owners or users of other mining pools have incentives to conduct DDoS attacks because it helps reduce the competition they face and potentially attract more miners to their pools. Opposition of Bitcoin, such as certain governments, banks, traditional payment processors may also attack. For a summary, see http://www.bitecoin.com/online/2015/01/11102.html.

these alternative channels are less likely to be the key drivers for the empirical patterns.[43] Crypto-mining represents a setting that products are not differentiated in the traditional sense. Products are differentiated in the sense that larger pools provide greater risk-sharing services, which our model accounts for. Larger pools enjoying larger trust may not be consistent with the fact that they have slower growth. Operation-wise, mining in a pool is not particularly easier than mining solo, if it is easier at all, so the industry maturing is unlikely to be the entire story.

# 7 Conclusion

Our paper's contribution is three-fold. First, we formally develop a theory of mining pools that highlights risk sharing as a natural centralizing force. When applied to proof-of-work-based blockchains, our theory reveals that financial innovations that improve risk sharing can escalate the mining arms race, increasing energy consumption. Second, we explain why a blockchain system could remain decentralized over time, and find empirical evidences from the Bitcoin mining industry that support our theory. Albeit not necessarily the only explanation for the industry evolution, ours closely ties to the risk-sharing benefit — the main driver for the emergence of mining pools in the first place. Our model therefore serves as a backbone upon which other external forces (e.g. DDoS attacks) could be added. Finally, our paper adds to the literature on industrial organization by incorporating the network effect of risk sharing into a monopolistic competition model and highlight in the context of cryptocurrency mining the roles of risks and fees in firm-size distribution.

As a first economics paper on mining pools, we have to leave many interesting topics to future research. For example, we do not take into account potential pool collusion or alternative pool objectives. Anecdotally, there is speculation that a large pool ViaBTC, along with allies AntPool and BTC.com pool, are behind the recent promotion of Bitcoin Cash, a competing cryptocurrency against Bitcoin. Hence these pools' behavior in Bitcoin mining may not necessarily be profit-maximizing. We also do not consider the ramification of concentration along the vertical value chain of mining. For instance, Bitmain, the owner of AntPool and BTC.com, as well partial owner of ViaBTC, is also the largest Bitcoin mining ASIC producer who currently controls 70% of world ASIC supply. Because we focus on pool

[43] We thank an anonymous referee for suggesting alternative channels and pointing out why they are unlikely the key drivers.

formation and competition, we leave open an orthogonal (geographic) dimension of mining power concentration: locations with cheap electricity, robust network, and cool climate tend to attract disproportionately more hash rates. In this regard, our findings constitute a first-order benchmark result rather than a foregone conclusion.

# References


Andrews, Dan, Chiara Criscuolo, Peter N Gal, et al., 2016, The best versus the rest: the global productivity slowdown, divergence across firms and the role of public policy, Discussion paper, OECD Publishing.

Autor, David, David Dorn, Lawrence F Katz, Christina Patterson, and John Van Reenen, 2017, Concentrating on the fall of the labor share, *The American Economic Review* 107, 180.

Beccuti, Juan, Christian Jaag, et al., 2017, The bitcoin mining game: On the optimality of honesty in proof-of-work consensus mechanism, Discussion paper, .

Benetton, Matteo, Giovanni Compiani, and Adair Morse, 2019, Cryptomining: Local evidence from china and the us, *Working paper*.

Berk, Jonathan B, and Richard C Green, 2004, Mutual fund flows and performance in rational markets, *Journal of political economy* 112, 1269–1295.

Berk, Jonathan B, Richard Stanton, and Josef Zechner, 2010, Human capital, bankruptcy, and capital structure, *The Journal of Finance* 65, 891–926.

Biais, Bruno, Christophe Bisiere, Matthieu Bouvard, and Catherine Casamatta, 2018, The blockchain folk theorem, .

Budish, Eric, 2018, The economic limits of bitcoin and the blockchain, Discussion paper, National Bureau of Economic Research.

Burdzy, Krzysztof, David M Frankel, and Ady Pauzner, 2001, Fast equilibrium selection by rational players living in a changing world, *Econometrica* 69, 163–189.

Calvo, Guillermo A, 1983, Staggered prices in a utility-maximizing framework, *Journal of monetary Economics* 12, 383–398.

Cao, Sean, Lin William Cong, and Baozhong Yang, 2018, Auditing and blockchains: Pricing, misstatements, and regulation, *Working Paper. Submission invited.*

Caves, Richard E, 1998, Industrial organization and new findings on the turnover and, *Journal of economic literature* 36, 1947–1982.

Chapman, James, Rodney Garratt, Scott Hendry, Andrew McCormack, and Wade McMahon, 2017, Project jasper: Are distributed wholesale payment systems feasible yet?, *Financial System* p. 59.

Chiu, Jonathan, and Thorsten V Koeppl, 2017, The economics of cryptocurrencies–bitcoin and beyond, .

——— , 2018, Blockchain-based settlement for asset trading, *Review of Financial Studies* Forthcoming.

Cong, Lin William, and Zhiguo He, 2018, Blockchain disruption and smart contracts, *Review of Financial Studies* Forthcoming.

Cong, Lin William, Ye Li, and Neng Wang, 2018, Tokenomics: Dynamic adoption and valuation, *BFI Working Paper*.

de Vilaca Burgos, Aldenio, Jose Deodoro de Oliveira Filho, Marcus Vinicius Cursino Suares, and Rafael Sarres de Almeida, 2017, Distributed ledger technical research in central bank of brazil, .

de Vries, Alex, 2019, Renewable energy will not solve bitcoins sustainability problem, *Joule* 3, 893–898.

Dimitri, Nicola, 2017, Bitcoin mining as a contest, *Ledger* 2, 31–37.

Easley, David, Maureen O'Hara, and Soumya Basu, 2017, From mining to markets: The evolution of bitcoin transaction fees, .

Economist, The, 2017, Learning the lessons of equihack, *The Economist September 16, 2017* September 16, 14.

Eyal, Ittay, 2015, The miner's dilemma, in *Security and Privacy (SP), 2015 IEEE Symposium on* pp. 89–103. IEEE.

——— , and Emin Gün Sirer, 2014, Majority is not enough: Bitcoin mining is vulnerable, in *International Conference on Financial Cryptography and Data Security* pp. 436–454. Springer.

Fama, Eugene F, 1976, *Foundations of finance: portfolio decisions and securities prices* (Basic Books (AZ)).

Fisch, Ben, Rafael Pass, and Abhi Shelat, 2017, Socially optimal mining pools, in *International Conference on Web and Internet Economics* pp. 205–218. Springer.

Gencer, Adem Efe, Soumya Basu, Ittay Eyal, Robbert van Renesse, and Emin Gün Sirer, 2018, Decentralization in bitcoin and ethereum networks, *arXiv preprint arXiv:1801.03998*.

Gervais, Arthur, Ghassan O Karame, Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf, and Srdjan Capkun, 2016, On the security and performance of proof of work blockchains, in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* pp. 3–16. ACM.

Glode, Vincent, Richard C Green, and Richard Lowery, 2012, Financial expertise as an arms race, *The Journal of Finance* 67, 1723–1759.

Harris, Milton, and Bengt Holmstrom, 1982, A theory of wage dynamics, *The Review of Economic Studies* 49, 315–333.

Harvey, Campbell R, 2016, Cryptofinance, *Working Paper*.

He, Zhiguo, and Wei Xiong, 2012, Dynamic debt runs, *Review of Financial Studies* 25, 1799–1843.

Hölmstrom, Bengt, 1979, Moral hazard and observability, *The Bell journal of economics* pp. 74–91.

Hortaçsu, Ali, and Chad Syverson, 2004, Product differentiation, search costs, and competition in the mutual fund industry: A case study of s&p 500 index funds, *The Quarterly Journal of Economics* 119, 403–456.

Huberman, Gur, Jacob D Leshno, and Ciamac C Moallemi, 2017, Monopoly without a monopolist: An economic analysis of the bitcoin payment system, .

Kiayias, Aggelos, Elias Koutsoupias, Maria Kyropoulou, and Yiannis Tselekounis, 2016, Blockchain mining games, in *Proceedings of the 2016 ACM Conference on Economics and Computation* pp. 365–382. ACM.

Konrad, Kai A, 2007, Strategy in contests-an introduction, *WZB-Markets and Politics Working Paper No. SP II* 1.

Kroll, Joshua A, Ian C Davey, and Edward W Felten, 2013, The economics of bitcoin mining, or bitcoin in the presence of adversaries, in *Proceedings of WEIS* vol. 2013. Citeseer.

Kugler, Logan, 2018, Why cryptocurrencies use so much energy: and what to do about it, *Communications of the ACM* 61, 15–17.

Lee, Sherman, 2018, Bitcoin's energy consumption can power an entire country – but eos is trying to fix that, Discussion paper, https://www.forbes.com/sites/shermanlee/2018/04/19/bitcoins-energy-consumption-can-power-an-entire-country-but-eos-is-trying-to-fix-that/#45c9a5e91bc8.

Li, Jiasun, 2015, Profit-sharing, wisdom of the crowd, and theory of the firm, *Discussion Paper*.

——— , 2017, Profit sharing: A contracting solution to harness the wisdom of the crowd, .

Li, Jingming, Nianping Li, Jinqing Peng, Haijiao Cui, and Zhibin Wu, 2019, Energy consumption of cryptocurrency mining: A study of electricity consumption in mining cryptocurrencies, *Energy* 168, 160–168.

Li, Jiasun, and William Mann, 2018, Initial coin offering and platform building, .

Ma, June, Joshua S Gans, and Rabee Tourky, 2018, Market structure in bitcoin mining, Discussion paper, National Bureau of Economic Research.

Malinova, Katya, and Andreas Park, 2016, Market design for trading with blockchain technology, *Available at SSRN*.

Mora, Camilo, Randi L Rollins, Katie Taladay, Michael B Kantar, Mason K Chock, Mio Shimada, and Erik C Franklin, 2018, Bitcoin emissions alone could push global warming above 2°c, *Nature Climate Change* p. 1.

Nakamoto, Satoshi, 2008, Bitcoin: A peer-to-peer electronic cash system, .

Nayak, Kartik, Srijan Kumar, Andrew Miller, and Elaine Shi, 2016, Stubborn mining: Generalizing selfish mining and combining with an eclipse attack, in *Security and Privacy (EuroS&P), 2016 IEEE European Symposium on* pp. 305–320. IEEE.

Nitzan, Shmuel, 1991, Collective rent dissipation, *The Economic Journal* 101, 1522–1534.

Pagnotta, Emiliano, and Andrea Buraschi, 2018, An equilibrium valuation of bitcoin and decentralized network assets, .

Prat, Julien, and Benjamin Walter, 2018, An equilibrium model of the market for bitcoin mining, .

Rogers, Adam, 2017, The hard math behind bitcoin's global warming problem, *WIRED* Dec 15, 2017, https://www.wired.com/story/bitcoin–global–warming/.

Rosenfeld, Meni, 2011, Analysis of bitcoin pooled mining reward systems, *arXiv preprint arXiv:1112.4980*.

Ross, Stephen A, 1999, Adding risks: Samuelson's fallacy of large numbers revisited, *Journal of Financial and Quantitative Analysis* 34, 323–339.

Rossi-Hansberg, Esteban, and Mark LJ Wright, 2007, Establishment size dynamics in the aggregate economy, *American Economic Review* 97, 1639–1666.

Saleh, Fahad, 2017, Blockchain without waste: Proof-of-stake, Discussion paper, working Paper.

Salop, Steven, and Joseph Stiglitz, 1977, Bargains and ripoffs: A model of monopolistically competitive price dispersion, *The Review of Economic Studies* 44, 493–510.

Samuelson, Paul A, 1963, Risk and uncertainty: A fallacy of large numbers, .

Sapirshtein, Ayelet, Yonatan Sompolinsky, and Aviv Zohar, 2015, Optimal selfish mining strategies in bitcoin, *arXiv preprint arXiv:1507.06183*.

——— , 2016, Optimal selfish mining strategies in bitcoin, in *International Conference on Financial Cryptography and Data Security* pp. 515–532. Springer.

Schrijvers, Okke, Joseph Bonneau, Dan Boneh, and Tim Roughgarden, 2016, Incentive compatibility of bitcoin mining pool reward functions, in *International Conference on Financial Cryptography and Data Security* pp. 477–498. Springer.

Stiglitz, Joseph E, 1974, Incentives and risk sharing in sharecropping, *The Review of Economic Studies* 41, 219–255.

Torpey, Kyle, 2016, An interview with viabtc, the new bitcoin mining pool on the blockchain, *Bitcoin Magazine* p. Sept 16.

Truby, Jon, 2018, Decarbonizing bitcoin: Law and policy choices for reducing the energy consumption of blockchain technologies and digital currencies, *Energy research & social science*.

Varian, Hal R, 1980, A model of sales, *The American Economic Review* 70, 651–659.

Vasek, Marie, Micah Thornton, and Tyler Moore, 2014, Empirical analysis of denial-of-service attacks in the bitcoin ecosystem, in *International Conference on Financial Cryptography and Data Security* pp. 57–71. Springer.

Vukolić, Marko, 2015, The quest for scalable blockchain fabric: Proof-of-work vs. bft replication, in *International Workshop on Open Problems in Network Security* pp. 112–125. Springer.

Wilson, Robert, 1968, The theory of syndicates, *Econometrica* pp. 119–132.

Yermack, David, 2017, Corporate governance and blockchains, *Review of Finance* p. rfw074.

# Appendix

## A Proofs of Lemmas and Propositions

### A1. Proof of Proposition 1

*Proof.* It is easy to verify that $\mathbb{E}[X_{pool}] = \mathbb{E}[X_{solo}]$. Hence it suffices to show that $X_{solo}$ is a mean-preserving spread of $X_{pool}$. To see this, note that

$$\begin{aligned} X_{solo} &= (\tilde{B}^A_{solo} + \tilde{B}^B_{solo})R - \tilde{B}^B_{solo}R \;=\; \tilde{B}_{pool}R - \tilde{B}^B_{solo}R \\ &= \frac{\lambda_A}{\lambda_A+\lambda_B}\tilde{B}_{pool}R + \frac{\lambda_B}{\lambda_A+\lambda_B}\tilde{B}_{pool}R - \tilde{B}^B_{solo}R \\ &= X_{pool} + \left(\frac{\lambda_B}{\lambda_A+\lambda_B}\tilde{B}_{pool}R - \tilde{B}^B_{solo}R\right), \text{ and} \\ &\mathbb{E}\left[\frac{\lambda_B}{\lambda_A+\lambda_B}\tilde{B}_{pool}R - \tilde{B}^B_{solo}R \mid X_{pool}\right] = 0, \end{aligned} \tag{18}$$

where $\tilde{B}^i_{solo}, i \in \{A, B\}$ denotes the number of blocks a miner/pool with hash rate $\lambda_i$ finds within time $T$. (18) holds because

$$\mathbb{E}\left[\frac{\lambda_B}{\lambda_A+\lambda_B}\tilde{B}_{pool}R - \tilde{B}^B_{solo}R \mid \tilde{B}_{pool} = n\right] = \frac{\lambda_B}{\lambda_A+\lambda_B}nR - \mathbb{E}\left[\tilde{B}^B_{solo} \mid \tilde{B}_{pool} = n\right]R, \text{ while}$$

$$\begin{aligned} \mathbb{E}\left[\tilde{B}^B_{solo} \mid \tilde{B}_{pool} = n\right] &= \mathbb{E}\left[\tilde{B}^B_{solo} \mid \tilde{B}^A_{solo} + \tilde{B}^B_{solo} = n\right] = \sum_{k=1}^{n} k \frac{\left(e^{-\lambda_B}\frac{\lambda_B^k}{k!}\right)\left(e^{-\lambda_A}\frac{\lambda_A^{n-k}}{(n-k)!}\right)}{e^{-(\lambda_A+\lambda_B)}\frac{(\lambda_A+\lambda_B)^n}{n!}} \\ &= \sum_{k=1}^{n} k \frac{n!}{k!(n-k)!}\left(\frac{\lambda_B}{\lambda_A+\lambda_B}\right)^k\left(\frac{\lambda_A}{\lambda_A+\lambda_B}\right)^{n-k} = \frac{\lambda_B}{\lambda_A+\lambda_B}n \end{aligned}$$

□

### A2. Proof of Proposition 2

*Proof.* We prove the more general case with potential entrant pools. We start with individual miner's problem in Eq. (10). With $\Lambda_{pm} = 0$, the derivative with respect to $\lambda_m$ is

$$\frac{1}{\Lambda}R(1-f_m)e^{-\rho R(1-f_m)\frac{\lambda_m}{\Lambda_{am}}} - C \tag{19}$$

Note that in a symmetric equilibrium, $\Lambda_{am} = N\lambda_m$. Therefore the marginal utility of adding hash rate to pool $m$ is simply

$$\frac{1}{\Lambda}R(1-f_m)e^{-\rho R(1-f_m)/N} - C \tag{20}$$

which is strictly monotone (either decreasing or increasing) in $f_m$ over $[0,1]$. Then an equilibrium must have $f_m$ being the same for all incumbent pools, for otherwise a miner can profitably deviate by moving some hash rate from one pool to another. If all incumbent pools are charging positive fees, then at least one pool owner can lower the fee by an infinitesimal amount to gain a non-trivial measure of hash rate, leading to a profitable deviation. Therefore, $f_m = 0 \ \forall \ m \in \{1, 2, \cdots, M^I\}$, where $M^I$ denotes the number of incumbent pools. We use $M$ to denote the total number of entrant and incumbent pools.

Now suppose we have entrants who can enter by paying $K$, they cannot possibly charge a positive fee because otherwise all miners would devote hash rate to incumbents who charge zero fees. Given that they are then indifferent between entering or not, any number of entrants could be an equilibrium outcome if $K = 0$. If $K$ is positive, they cannot enter and recoup the setup cost.

Now for individual miners to be indifferent between acquiring more hash rate or not, the global hash rate $\Lambda$ has to equalize the marginal benefit of hash rate with its marginal cost $C$, which leads to $\Lambda = \frac{R}{C} e^{-\rho R/N}$. Therefore the payoff to each miner is

$$\frac{1}{\rho\Lambda}\left[\sum_{m=0}^{M} \Lambda_{am}\left(1 - e^{-\rho R \frac{\lambda_m}{\Lambda_{am}}}\right)\right] - \frac{R}{N} e^{-\rho R/N} = \frac{1}{\rho}(1 - e^{-\rho R/N}) - \frac{R}{N} e^{-\rho R/N}, \tag{21}$$

where we have used the fact that $\sum_{m=0}^{M} \Lambda_{am} = \Lambda$, the sum of all hash rates of active miners in consideration with an aggregate measure $N$. And the utility from mining in pools is strictly positive, as it is easy to show that RHS is strictly positive when $R > 0$. So miners indeed join these pools. The exact distribution of pool size does not matter as long as $\sum_{m=0}^{M} \lambda_m = \Lambda/N = \frac{R}{NC} e^{-\rho R/N}$. □

## A3. Proof of Proposition 3

*Proof.* Obviously, for pools charging the same $f_m$, the RHS of (14) is the same, implying $\frac{\lambda_m^*}{\Lambda_{pm}}$ is the same. Now, because of free entry of mining (fully flexible hash rate acquisition), in equilibrium (13) implies that

$$R(1 - f_m) = C\Lambda e^{\rho R(1-f_m)\frac{\lambda_m}{\Lambda_{am}+\Lambda_{pm}}} \leq C\Lambda e^{\rho R(1-f_m)/N} < C\Lambda e, \tag{22}$$

where the last inequality follows from Assumption 1. This implies that the RHS of (14), if positive, has negative partial derivative w.r.t. $f_m$. Therefore, among pools having positive active mining, a pool charging a higher fee would have a smaller net growth $\frac{\lambda_m}{\Lambda_{pm}}$ in equilibrium.

□

## A4. Proof of Proposition 4

The following lemmas are useful for the proof of Proposition 4.

**Lemma 1.** $1 - \frac{N}{\rho R(1-f_m^*)} \ln \frac{R(1-f_m^*)}{C\Lambda^*} > 0$.

*Proof.* Proof by contradiction. Suppose otherwise, then

$$C\Lambda^* \leq R(1-f_m^*)e^{-\frac{\rho R(1-f_m^*)}{N}} < R(1-f_m^*)e^{-\rho R(1-f_m^*)\frac{\Lambda_{am}^*}{N(\Lambda_{am}^*+\Lambda_{pm})}} \leq C\Lambda^*.$$

Notice that the last inequality comes from active miner's FOC. □

**Lemma 2.** *$\forall m \in \{1, \cdots, M\}$, if $1 \geq \frac{1}{1-\frac{N}{\rho R(1-f_m^*)}\ln\frac{R(1-f_m^*)}{C\Lambda^*}}$ then $f_m^* = 1$.*

*Proof.* When $1 \geq \frac{1}{1-\frac{N}{\rho R(1-f_m^*)}\ln\frac{R(1-f_m^*)}{C\Lambda^*}}$, $f_m^*$ lies in an interval $\mathcal{F} \subseteq [0,1]$ where $\Lambda_m = \Lambda_{pm}$. Within $\mathcal{F}$, $\Lambda = \Lambda^*$ is unaffected by unilateral changes to $f_m$. Hence $f_m^* = \text{argmax}_{\mathcal{F}} \frac{1-e^{-\rho R f_m}}{\Lambda^*} = 1$. □

This lemma simply confirms that managers either charge an interior fee or charge the highest fee and get no active miner. Therefore, when focusing on pools that grow, we only need to examine those charging interior fees.

**Lemma 3.** *$\forall m$ s.t. $f_m < 1$, pool owners' FOC holds in equilibrium:*

$$\rho R e^{-\rho R f_m}\left(1-\frac{N}{\rho R(1-f_m)}\ln\frac{R(1-f)}{C\Lambda}\right) - \left(1-e^{-\rho R f_m}\right)\frac{N}{\rho R(1-f_m)^2}\left(1-\ln\frac{R(1-f)}{C\Lambda}\right)$$
$$- \left(1-e^{-\rho R f_m}\right)\frac{\frac{\left(1-\frac{N}{\rho R(1-f_m)}\ln\frac{R(1-f)}{C\Lambda}+\frac{N}{\rho R(1-f_m)}\right)}{\left(1-\frac{N}{\rho R(1-f_m)}\ln\frac{R(1-f_m)}{C\Lambda}\right)^2}\frac{N}{\rho R(1-f_m)^2}(\ln\frac{R(1-f_m)}{C\Lambda}-1)\Lambda_{pm}}{\Lambda + \sum_{m'\in\mathcal{M}_1}\frac{\frac{N}{\rho R(1-f_{m'})}}{\left(1-\frac{N}{\rho R(1-f_{m'})}\ln\frac{R(1-f_{m'})}{C\Lambda}\right)^2}\Lambda_{pm'}} = 0, \tag{23}$$

*where set $\mathcal{M}_1$ is so defined that $\forall m \in \mathcal{M}_1, f_m^* < 1$.*

*Proof.* Substitute

$$\frac{d\Lambda}{df_m} = -\frac{\frac{\partial}{\partial f_m}\left(\Lambda - \frac{1}{1-\frac{N}{\rho R(1-f_m)}\ln\frac{R(1-f_m)}{C\Lambda}}\Lambda_{pm} - \Lambda_{-m}\right)}{\frac{\partial}{\partial\Lambda}\left(\Lambda - \frac{1}{1-\frac{N}{\rho R(1-f_m)}\ln\frac{R(1-f_m)}{C\Lambda}}\Lambda_{pm} - \Lambda_{-m}\right)} = \frac{\frac{1}{\left(1-\frac{N}{\rho R(1-f_m)}\ln\frac{R(1-f_m)}{C\Lambda}\right)^2}\frac{N}{\rho R(1-f_m)^2}(\ln\frac{R(1-f_m)}{C\Lambda}-1)\Lambda_{pm}}{1+\sum_{m'\in\mathcal{M}_1}\frac{\frac{N}{\rho R(1-f_{m'})}}{\Lambda\left(1-\frac{N}{\rho R(1-f_{m'})}\ln\frac{R(1-f_{m'})}{C\Lambda}\right)^2}\Lambda_{p'm}}$$

into the derivative of pool $m$'s objective $\Lambda_{pm}\frac{1-e^{-\rho R f_m}}{\Lambda\left(1-\frac{N}{\rho R(1-f_m)}\ln\frac{R(1-f_m)}{C\Lambda}\right)}$ with respect to $f_m$:

$$\Lambda_{pm}\left(\frac{\rho R e^{-\rho R f_m}}{\Lambda\left(1-\frac{N}{\rho R(1-f_m)}\ln\frac{R(1-f)}{C\Lambda}\right)} - \frac{\left(1-e^{-\rho R f_m}\right)\frac{N}{\rho R(1-f_m)^2}\left(1-\ln\frac{R(1-f)}{C\Lambda}\right)}{\Lambda\left(1-\frac{N}{\rho R(1-f_m)}\ln\frac{R(1-f)}{C\Lambda}\right)^2}\right.$$
$$\left. - \frac{\left(1-e^{-\rho R f_m}\right)\left(1-\frac{N}{\rho R(1-f_m)}\ln\frac{R(1-f)}{C\Lambda}+\frac{N}{\rho R(1-f_m)}\right)}{\Lambda^2\left(1-\frac{N}{\rho R(1-f_m)}\ln\frac{R(1-f)}{C\Lambda}\right)^2}\frac{d\Lambda}{df_m}\right),$$

and factor out nonzero terms. □

*Proof of Proposition 4.* We prove the proposition by contradiction. Suppose a larger pool charges a weakly lower fee. From (23) in Lemma 3, we know that $\forall m$ s.t. $f_m < 1$

$$\frac{\Lambda_{pm}}{\Lambda^* + \sum_{m' \in \mathcal{M}_1} \frac{\frac{N}{\rho R(1-f'^*_m)}}{\left(1-\frac{N}{\rho R(1-f'^*_m)} \ln \frac{R(1-f'^*_m)}{C\Lambda^*}\right)^2} \Lambda_{pm'}} = \tag{24}$$
$$\frac{\left(1-\frac{N}{\rho R(1-f^*_m)} \ln \frac{R(1-f^*_m)}{C\Lambda^*}\right)^2}{\left(1-\frac{N}{\rho R(1-f^*_m)} \ln \frac{R(1-f^*_m)}{C\Lambda^*} + \frac{N}{\rho R(1-f^*_m)}\right)} \left(1 - \frac{\rho^2 R^2 (1-f^*_m)^2 e^{-\rho R f^*_m} \left(1-\frac{N}{\rho R(1-f^*_m)} \ln \frac{R(1-f^*_m)}{C\Lambda^*}\right)}{(1-e^{-\rho R f^*_m}) N \left(1 - \ln \frac{R(1-f^*_m)}{C\Lambda^*}\right)}\right).$$

Because the left hand side of (24) strictly increases in $\Lambda_{pm}$ (its numerator equals $\Lambda_{pm}$ and denominator is independent of $m$), to arrive at a contradiction, we only need to show that the RHS of (24) as a function of $f^*_m$ (keeping $\Lambda^*$ fixed because we are doing a cross-section comparison across pools) is increasing, i.e.

$$\frac{\partial}{\partial f}\left[\frac{\left(1-\frac{N}{\rho R(1-f)} \ln \frac{R(1-f)}{C\Lambda^*}\right)^2}{\left(1-\frac{N}{\rho R(1-f)} \ln \frac{R(1-f)}{C\Lambda^*} + \frac{N}{\rho R(1-f)}\right)} \left(1 - \frac{\rho^2 R^2 (1-f)^2 e^{-\rho R f} \left(1-\frac{N}{\rho R(1-f)} \ln \frac{R(1-f)}{C\Lambda^*}\right)}{(1-e^{-\rho R f}) N \left(1 - \ln \frac{R(1-f)}{C\Lambda^*}\right)}\right)\right] > 0. \tag{25}$$

This is true because we can prove a set of stronger results:

$$\frac{\partial}{\partial f}\left[\frac{\left(1-\frac{N}{\rho R(1-f)} \ln \frac{R(1-f)}{C\Lambda^*}\right)}{\left(1-\frac{N}{\rho R(1-f)} \ln \frac{R(1-f)}{C\Lambda^*} + \frac{N}{\rho R(1-f)}\right)}\right] > 0, \text{ and} \tag{26}$$
$$\frac{\partial}{\partial f}\left[\left(1-\frac{N}{\rho R(1-f)} \ln \frac{R(1-f)}{C\Lambda^*}\right)\left(1 - \frac{\rho^2 R^2 (1-f)^2 e^{-\rho R f}\left(1-\frac{N}{\rho R(1-f)} \ln \frac{R(1-f)}{C\Lambda^*}\right)}{\left(1-e^{-\rho R f}\right) N \left(1-\ln \frac{R(1-f)}{C\Lambda^*}\right)}\right)\right] > 0. \tag{27}$$

To see this, notice that the left hand side of (26) is

$$\frac{\frac{N}{(1-f)^2\rho R} - \frac{N \ln\left(\frac{(1-f)R}{c\Lambda^*}\right)}{(1-f)^2\rho R}}{-\frac{N \ln\left(\frac{(1-f)R}{c\Lambda^*}\right)}{(1-f)\rho R} + \frac{N}{(1-f)\rho R} + 1} - \frac{\left(\frac{2N}{(1-f)^2\rho R} - \frac{N \ln\left(\frac{(1-f)R}{c\Lambda^*}\right)}{(1-f)^2\rho R}\right)\left(1 - \frac{N \ln\left(\frac{(1-f)R}{c\Lambda^*}\right)}{(1-f)\rho R}\right)}{\left(-\frac{N \ln\left(\frac{(1-f)R}{c\Lambda^*}\right)}{(1-f)\rho R} + \frac{N}{(1-f)\rho R} + 1\right)^2} \tag{28}$$
$$= \frac{N\left(\frac{N}{(1-f)\rho R} - 1\right)}{(1-f)^2 \rho R \left(-\frac{N \ln\left(\frac{(1-f)R}{C\Lambda^*}\right)}{(1-f)\rho R} + \frac{N}{(1-f)\rho R} + 1\right)^2}, \tag{29}$$

which is positive when $N > (1-f)\rho R$, which always holds because $N > \rho R$ (Assumption 1).

Meanwhile, the left hand side of (27) is

$$\left( \frac{(1-f)^2 R^3 \rho^3 e^{f\rho R} \left(1 - \frac{N \ln\left(\frac{(1-f)R}{c\Lambda^*}\right)}{(1-f)\rho R}\right)}{N\left(e^{f\rho R}-1\right)^2 \left(1-\ln\left(\frac{(1-f)R}{c\Lambda^*}\right)\right)} - \frac{(1-f)^2\rho^2 R^2 \left(\frac{N}{(1-f)^2\rho R} - \frac{N\ln\left(\frac{(1-f)R}{c\Lambda^*}\right)}{(1-f)^2\rho R}\right)}{N\left(e^{f\rho R}-1\right)\left(1-\ln\left(\frac{(1-f)R}{c\Lambda^*}\right)\right)} \right.$$

$$\left. + \frac{2(1-f)\rho^2 R^2 \left(1 - \frac{N\ln\left(\frac{(1-f)R}{c\Lambda^*}\right)}{(1-f)\rho R}\right)}{N\left(e^{f\rho R}-1\right)\left(1-\ln\left(\frac{(1-f)R}{c\Lambda^*}\right)\right)} + \frac{(1-f)\rho^2 R^2 \left(1 - \frac{N\ln\left(\frac{(1-f)R}{c\Lambda^*}\right)}{(1-f)\rho R}\right)}{N\left(e^{f\rho R}-1\right)\left(1-\ln\left(\frac{(1-f)R}{c\Lambda^*}\right)\right)^2} \right) \times \left(1 - \frac{N\ln\left(\frac{(1-f)R}{c\Lambda^*}\right)}{(1-f)\rho R}\right)$$

$$+ \left(\frac{N}{(1-f)^2\rho R} - \frac{N\ln\left(\frac{(1-f)R}{c\Lambda^*}\right)}{(1-f)^2\rho R}\right) \left(1 - \frac{(1-f)^2\rho^2 R^2 \left(1 - \frac{N\ln\left(\frac{(1-f)R}{c\Lambda^*}\right)}{(1-f)\rho R}\right)}{N\left(e^{f\rho R}-1\right)\left(1-\ln\left(\frac{(1-f)R}{c\Lambda^*}\right)\right)}\right), \tag{30}$$

which is equal to

$$\frac{A\left(1 - \frac{N\ln\left(\frac{(1-f)R}{C\Lambda^*}\right)}{(1-f)\rho R}\right)^2 + \left(\frac{N\sqrt{e^{f\rho R}-1}\left(1-\ln\left(\frac{(1-f)R}{C\Lambda^*}\right)\right)}{(1-f)\sqrt{\rho R}} - \frac{(1-f)\sqrt{R^3\rho^3}(N-(1-f)\rho R)\left(1-\frac{N\ln\left(\frac{(1-f)R}{C\Lambda^*}\right)}{(1-f)\rho R}\right)}{N\sqrt{e^{f\rho R}-1}\left(1-\ln\left(\frac{(1-f)R}{C\Lambda^*}\right)\right)}\right)^2}{N\left(e^{f\rho R}-1\right)\left(1-\ln\left(\frac{(1-f)R}{C\Lambda^*}\right)\right)}, \tag{31}$$

where $A = \frac{(1-f)\rho^2 R^2}{N^2\left(e^{f\rho R}-1\right)\left(1-\ln\left(\frac{(1-f)R}{C\Lambda^*}\right)\right)^2} \times \left((1-f)N^2\rho R\left(e^{f\rho R}-1\right)\left(1-\ln\left(\frac{(1-f)R}{C\Lambda^*}\right)\right)^2 + \right.$

$$\left. N^2\left(e^{f\rho R}-1\right)\left(1-\ln\left(\frac{(1-f)R}{C\Lambda^*}\right)\right) + (1-f)^2\rho^2 R^2\left(N\left(1-\ln\left(\frac{(1-f)R}{C\Lambda^*}\right)\right) + N - (1-f)\rho R\right)\left(1 - \frac{N\ln\left(\frac{(1-f)R}{C\Lambda^*}\right)}{(1-f)\rho R}\right)\right). \tag{32}$$

$A > 0$ when $N > (1-f)\rho R$, which always holds because $N > \rho R$ (Assumption 1). Notice that for equilibrium $\{f_m^*\}$, Assumption 1 and Lemma 1 imply that the denominator of (31) is also positive. We conclude that (31) (and thus (27)) is positive. □

## A5. Proof of Proposition 5

*Proof.* First, we prove by contradiction that in equilibrium at most one pool enters. Suppose otherwise, then by a Bertrand argument all entrant pools charge zero fees, which would not render enough revenues with certainty equivalent exceeding the cost $K$. A contradiction.

Given that at most one new pools enters, we argue that in equilibrium the new pool must be collecting a certainty equivalent of $K$. If the pool collects more than $K$, then another potential pool owner can deviate to enter and charge a lightly lower fee to make a positive net profit; if the

pool owner collects less than $K$, then it has a profitable deviation to not enter at all.

Denote the fee charged by the entry pool by $f_E$, we have the following lemma.

**Lemma 4** (Pool Entry)**.** *There exists a strictly positive cutoff $\hat{K} > 0$ such that when $K > \hat{K}$, no new pool enters. When $0 < K \leq \hat{K}$, at most one pool enters, charging an endogenous fee $f_E$ so that it collects an certainty equivalent of $K$.*

*Proof.* Suppose this new entrant pool owner charges $f_E$, the marginal benefit of allocating hash rate to the pool is $\frac{1}{\Lambda}R(1-f_E)e^{-\rho R(1-f_E)\frac{\lambda_E}{\Lambda_{aE}}} = \frac{1}{\Lambda}R(1-f_E)e^{-\rho R(1-f_E)/N}$. If $\Lambda$ were so large that this is less than the marginal cost $C$, no active miner joins which contradicts the new pool owner's entry decision. Therefore, in an equilibrium with new pool entry, $f_E$ uniquely pins down $\Lambda$,

$$\Lambda = \frac{1}{C}R(1-f_E)e^{-\rho R(1-f_E)/N}, \tag{33}$$

and

$$\Lambda \geq \sum_{m=1}^{M^I}(\Lambda_{am}+\Lambda_{pm}) = \sum_{m=1}^{M^I}\max\left\{\Lambda_{pm}, \frac{\rho R(1-f_m)\Lambda_{pm}}{\rho R(1-f_m)+N\ln[C\Lambda]-N\ln[R(1-f_m)]}\right\}, \tag{34}$$

where the last equality follows from (14).

In fact, pool owners choose fees to maximize

$$\Lambda_{pm}\cdot\frac{1-e^{-\rho R f_m}}{\rho\Lambda}\left[1+\max\left\{0, \frac{N\ln[R(1-f_m)]-N\ln[C\Lambda]}{\rho R(1-f_m)+N\ln[C\Lambda]-N\ln[R(1-f_m)]}\right\}\right]. \tag{35}$$

We note that this optimization completely separates $\Lambda_{pm}$ and $f_m$. Therefore, the optimal fee charged by all pools are the same and is independent of $\Lambda_{pm}$, which we denote by $f_I(\Lambda)$. Then (34) simplifies to

$$\Lambda \geq \left(\sum_{m=1}^{M^I}\Lambda_{pm}\right)\max\left\{1, \frac{\rho R(1-f_I)}{\rho R(1-f_I)+N\ln[C\Lambda]-N\ln[R(1-f_I)]}\right\}, \tag{36}$$

The entrant derives a utility of

$$\begin{aligned} u_E(f_E) &\equiv \frac{\Lambda_{aE}(f_E)}{\rho\Lambda(f_E)}\left(1-e^{-\rho R f_E}\right) = \frac{\Lambda(f_E)-\sum_{m=1}^{M^I}(\Lambda_{am}+\Lambda_{pm})}{\rho\Lambda(f_E)}\left(1-e^{-\rho R f_E}\right) \qquad (37)\\ &= \frac{\left(1-e^{-\rho R f_E}\right)}{\rho\Lambda(f_E)}\left[\Lambda(f_E)-\left(\sum_{m=1}^{M^I}\Lambda_{pm}\right)\max\left\{1, \frac{\rho R(1-f_I)}{\rho R(1-f_I)+N\ln[C\Lambda(f_E)]-N\ln[R(1-f_I)]}\right\}\right] \end{aligned}$$

We note that the expression is continuous and well-behaved in $f_E$, and its optimization over the bounded support $f_E \in [0,1]$ subject to the constraint of (36) has a maximum that is bounded above

by $\frac{1}{\rho}\left(1-e^{-\rho R}\right)$. We denote the maximum by

$$u(\hat{K}) \equiv \max_{f_E} u_E(f_E). \tag{38}$$

For $K > \hat{K}$, no new pool enters because an owner cannot recover the entry cost $K$; for $K \leq \hat{K}$, a new pool owner enters and charges an $f_E$ such that the certainty equivalence from the mining revenue exactly equals $K$. Again due to the continuity of (37) in $f_E$ and the fact that (37) attains zero when $f_E = 0$, for any $K \leq \hat{K}$ there exists a feasible fee $f_E$ the entrant can charge in equilibrium to recoup the entry cost $K$. The break-even condition for the entrant pool is exactly

$$\frac{\left(1-e^{-\rho R f_E}\right)}{\rho\Lambda(f_E)}\left[\Lambda(f_E) - \left(\sum_{m=1}^{M^I}\Lambda_{pm}\right)\max\left\{1, \frac{\rho R(1-f_I)}{\rho R(1-f_I) + N\ln[C\Lambda] - N\ln[R(1-f_I)]}\right\}\right] = u(K) \tag{39}$$

This said, it could be the case that for such an $f_E$, the incumbents charge fees to attract active hash rate exceeding the supposedly fixed $\Lambda$, which implies this would not be an equilibrium. As such, when $K$ is sufficiently small, there could be entry, but entry is not guaranteed in general.

□

The extreme case of $K = 0$ could in principal result in an arbitrary number of new pools, but the equilibrium allocation is equivalent to only one entry pool (one can combine all entry pools with zero fees into one as shown in Proposition 2).

The lemma tells us that there are only two situations we need to examine: (1) with sufficiently high $K$, there is no entry and we have $M = M^I$ pools; otherwise, (2) we have $M = M^I + 1$ pools, with a global hash rate determined by the entrant pool's fee charged to break even, taking the equilibrium fees charged by other pools as given.

We can characterize the resulting equilibrium of $K = 0$ in a fairly clean way. The global hash rates are pinned down by setting $f_E = 0$ in Eq. (33), so that $\Lambda = \frac{R}{C}e^{-\rho R/N}$. Given this, maximizing Eq. (16) gives the strictly positive equilibrium fee $f_I(\Lambda)$ charged by all incumbent pools. This fee in turn pins down the hash rates going to the incumbent pools, and the rest is attracted by the entry pool. We note that the equilibrium risk-sharing allocation is distorted by the strictly positive fees $f_I(\Lambda) > 0$ charged incumbent pools, which inefficiently pushes more active hash rates toward the zero-fee entry pool relative to the optimal risk sharing benchmark (absent fees).

Without new pool entry, the maximum global hash rate satisfies

$$\Lambda = \left(\sum_{m=1}^{M^I}\Lambda_{pm}\right)\frac{\rho R}{\rho R + N\ln[C\Lambda] - N\ln R} \tag{40}$$

Therefore, for sufficiently low $\sum_{m=1}^{M^I}\Lambda_{pm}$, the marginal benefit of allocating $\lambda_m$ to a pool charging zero fee is $\frac{1}{\Lambda}Re^{-\rho R\frac{\lambda_m}{\Lambda_{am}+\Lambda_{pm}}}$ exceeds the marginal cost $C$, so the pool owner can always charge a

positive fee and get a positive measure of active hash rate.

Now with new pool entry, suppose an incumbent pool charges zero fees, then the marginal benefit of allocating some hash rate to it satisfies the following when $\lambda_m$ is sufficiently small.

$$\frac{R}{\Lambda}e^{-\rho R\frac{\lambda_m}{N\lambda_m+\Lambda_{pm}}} > \frac{R}{\Lambda}e^{-\rho R\frac{1-f_E}{N}} = \frac{C}{1-f_E} > C \tag{41}$$

Therefore, in equilibrium there is always positive allocation to the incumbent pool. As such, the pool owner can always charge a positive pool fee and still gets positive measure of active hash rate.

Now with free entry, $f_E = 0$ in equilibrium, and $\Lambda = \frac{R}{C}e^{-\rho R/N}$. Because incumbents charge positive fees, the active miners do not allocate as many hash rates to them as in the full risk-sharing case.

□

# B A List of Mining Pool Fee Types

Source: Bitcoin Wiki.

- CPPSRB: Capped Pay Per Share with Recent Backpay.
- DGM: Double Geometric Method. A hybrid between PPLNS and Geometric reward types that enables to operator to absorb some of the variance risk. Operator receives portion of payout on short rounds and returns it on longer rounds to normalize payments.
- ESMPPS: Equalized Shared Maximum Pay Per Share. Like SMPPS, but equalizes payments fairly among all those who are owed.
- POT: Pay On Target. A high variance PPS variant that pays on the difficulty of work returned to pool rather than the difficulty of work served by pool.
- PPLNS: Pay Per Last N Shares. Similar to proportional, but instead of looking at the number of shares in the round, instead looks at the last N shares, regardless of round boundaries.
- PPLNSG: Pay Per Last N Groups (or shifts). Similar to PPLNS, but shares are grouped into shifts which are paid as a whole.
- PPS: Pay Per Share. Each submitted share is worth certain amount of BC. Since finding a block requires shares on average, a PPS method with 0
- PROP: Proportional. When block is found, the reward is distributed among all workers proportionally to how much shares each of them has found.
- RSMPPS: Recent Shared Maximum Pay Per Share. Like SMPPS, but system aims to prioritize the most recent miners first.
- SCORE: Score based system: a proportional reward, but weighed by time submitted. Each submitted share is worth more in the function of time t since start of current round. For each share score is updated by: score += exp(t/C). This makes later shares worth much more than earlier shares, thus the miners score quickly diminishes when they stop mining on the pool. Rewards are calculated proportionally to scores (and not to shares). (at slushs pool C=300 seconds, and every hour scores are normalized)
- SMPPS: Shared Maximum Pay Per Share. Like Pay Per Share, but never pays more than the pool earns.

Table 3: **Selected Pool Reward Contracts**

| **Name** | **Reward Type** | **Transaction fees** | **Prop. Fee** | **PPS Fee** |
|---|---|---|---|---|
| AntPool | PPLNS & PPS | kept by pool | 0% | 2.50% |
| BTC.com | FPPS | shared | 4% | 0% |
| BCMonster.com | PPLNS | shared | 0.50% | |
| Jonny Bravo's | PPLNS | shared | 0.50% | |
| Slush Pool | Score | shared | 2% | |
| BitMinter | PPLNSG | shared | 1% | |
| BTCC Pool | PPS | kept by pool | | 2.00% |
| BTCDig | DGM | kept by pool | 0% | |
| btcmp.com | PPS | kept by pool | | 4% |
| Eligius | CPPSRB | shared | 0% | |
| F2Pool | PPS | kept by pool | | 3% |
| GHash.IO | PPLNS | shared | 0% | |
| Give Me COINS | PPLNS | shared | 0% | |
| KanoPool | PPLNSG | shared | 0.90% | |
| Merge Mining Pool | DGM | shared | 1.50% | |
| Multipool | Score | shared | 1.50% | |
| P2Pool | PPLNS | shared | 0% | |
| MergeMining | PPLNS | shared | 1% | |

**Source**: Bitcoin wiki