Decentralized Mining in Centralized Pools*

Lin William Cong† Zhiguo He‡ Jiasun Li§

First draft: March 2018. Current draft: November 2018.

Abstract

An open blockchain's well-functioning relies on adequate decentralization, yet the rise of mining pools that provide risk-sharing leads to centralization, calling into question the viability of such systems. We show that mining pools as a financial innovation significantly exacerbates the arms race and thus energy consumption for proof-of-work-based blockchains. Moreover, cross-pool diversification and endogenous pool fees generally sustain decentralization — dominant pools better internalize the mining externality, charge higher fees, attract disproportionately less miners, and thus grows more slowly. Consequently, aggregate growth in mining pools is not accompanied by over-concentration of pools. Empirical evidence from Bitcoin mining supports our model predictions, and the economic insight applies to other blockchain protocols and industries sharing similar characteristics.

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

Keywords: Arms Race, Bitcoin, Blockchain, Climate Change, Cryptocurrency, Energy Consumption, Financial Innovation, FinTech, Mining Pools, PoW, Risk-Sharing.

*We thank Foteini Baldimtsi, Joseph Bonneau, Matthieu Bouvard, Bhagwan Chowdhry, Ye Li, Maureen O'Hara, Katrin Tinn, Liyan Yang, and David Yermack for helpful discussions; Zhenping Wang, Xiao Yin, and Xiao Zhang provided excellent research assistance. They also thank seminar and conference participants at Princeton, Chicago Booth, Columbia Business School, Cornell, CUNY Baruch, NYU Stern, Michigan Ross, George Mason, PBC School of Finance, Ant Financial, Yale SOM, Rice University, University of Houston, University of Maryland, Cleveland Fed, Indian School of Business, DataYes & ACM KDD China FinTech×AI Workshop, Summer Institute of Finance Conference, CEPR Gerzensee ESSFM Corporate Finance Workshop, China International Forum on Finance and Policy, NFA Conference, BFI Conference on Cryptocurrencies and Blockchains, and FinTech, Credit and the Future of Banking Conference (Rigi Kaltbad) for helpful comments and discussions. The authors are 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 University.

†University of Chicago Booth School of Business. Email: will.cong@chicagobooth.edu

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

§George Mason University School of Business. 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)).A majority of extant blockchains rely on variants of the proof-of-work (PoW) protocol, 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 with native crypto-tokens.[1] Miners have incentives to honestly record transactions because their rewards are only valid if their records are endorsed by subsequent miners.

Compared to a centralized system, blockchains have advantages such as robustness to cyber-attacks and avoidance of "single point of failure."[2] However, these benefits are predicated on adequate decentralization and the system's long-term sustainability, which is only a *technological* possibility, not a guaranteed *economic* reality. For one, practitioners and academics all recognize the egregious energy consumption in cryptocurrency mining, which is essentially an arms race that can cause great climate and environmental damage.[3] Moreover, Whereas Nakamoto (2008) envisions a perfect competition among independent computer nodes dispersed across the world, many cryptocurrencies witness the rise of "pooled mining" wherein miners partner together and share mining rewards, as opposed to "solo mining" wherein each miner bears all her own mining risks.

Figure 1 illustrates these phenomena with the Bitcoin data. Bitcoin mining pools have been gradually encroaching, constituting only 5% of the global hash rates (a measure of computation power) in June 2011 but almost 100% since late 2015. Intriguingly, the rise of

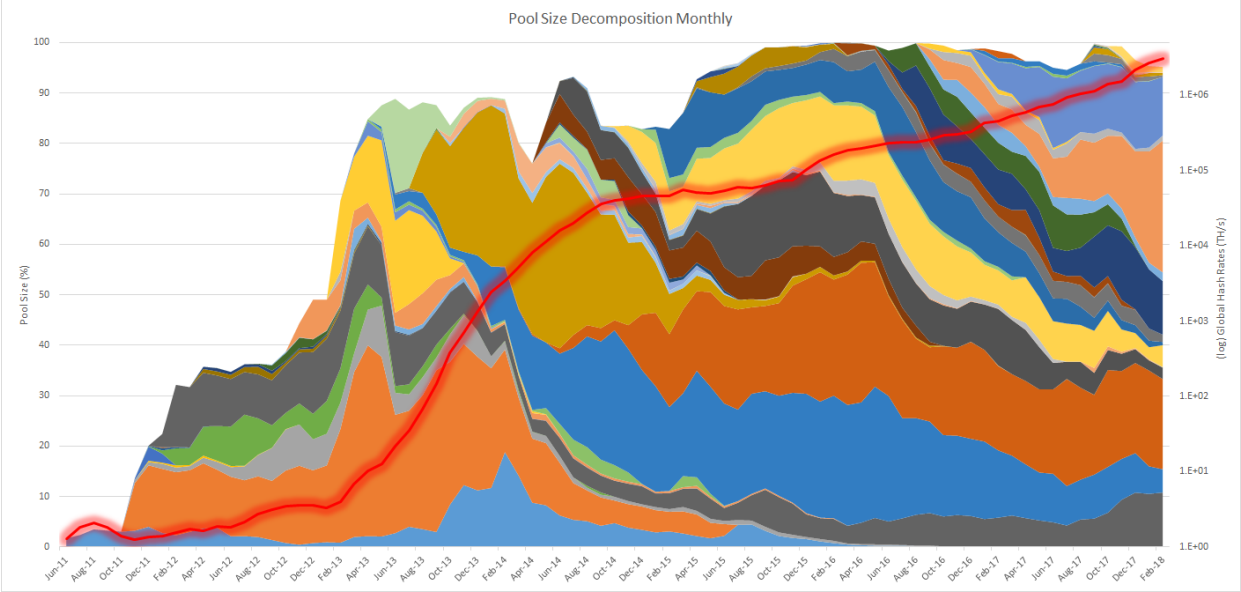
[1] Other protocols for decentralized consensus include Proof-of-Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), etc. We extend our discussion to PoS in Section 6.3. See also Saleh (2017) regarding the sustainability of PoS.

[2] Recent cyber scandals at Equifax offers a vivid lesson. See, e.g., Economist (2017). Blockchains are also presumably less vulnerable to misbehaviors and monopoly powers 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.

[3] As of April 2018, aggregate electricity devoted to Bitcoin mining alone exceeds 60 TWh, roughly the annual energy consumed by Switzerland as a country (Lee, 2018). The cryptocurrency forum Digiconomist provides similar estimates and points out that the mining of a single block consumes enough energy to power more than 28 U.S. homes for a full day, and is mostly fueled by coal-based electricity available at very low rates (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, its emissions alone 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 dominated by mining pools, but no pool seems ever to dominate the mining industry. The pool hash rates information comes from Bitcoinity and BTC.com). For more details, see Section 5.



mining pools coincides with the explosive growth in the global hash rates (plotted in red line, in log scale). While some pools gained significant shares at times, which calls into question whether a blockchain system can stay decentralized, none of the large pools that emerge at times has snowballed to dominance for prolonged periods of time.[4] Instead, pool sizes seem to exhibit a mean reverting tendency, hinting at concurrent economic forces suppressing over-centralization.

We argue that from an economic perspective, forming centralized pools in these supposedly decentralized systems is natural, because partnerships/cooperatives offer the most common organization forms in humans history for risk sharing among individual agents (e.g., the insurance industry). More importantly, we highlight for the first time that the enormous amount of energy devoted to cryptocurrency mining can be largely attributed to the rise of mining pools, which, as a financial innovation that provides better risk-sharing, significantly exacerbates the arms race associated with proof-of-work-based blockchains. Under

[4]One oft-discussed example is the mining pool GHash.io which briefly reached more than 51% of global hash rates in July, 2014.

reasonable model parameters, mining pools can easily multiply the global computation power devoted to mining by more than five times.

In contrast with this serious energy concern, we find that the winner-pool-take-all concern is somewhat misguided because cross-pool diversification and endogenous pool fees can sustain decentralization under general blockchain consensus protocols (PoW and alternative ones such as Proof-of-Stake (PoS) protocols). These insights are not only informative to the blockchain community, but also fundamental to our understanding of industrial organization and the trade-offs in decentralized versus centralized systems (e.g., Hayek (1945)), which becomes increasingly important as many industries transition into gig economies with on-demand workforce.

Specifically, we model the decision-making of miners in acquiring hash rates and allocating them into mining pools, together with the competition of pool managers who set fees for their risk-diversification services. We emphasize two particularly relevant characteristics of cryptocurrency mining. First, profit-driven miners face little transaction cost to participate in multiple mining pools, because switching between pools involves simply changing one parameter in the mining script. This contrasts with the literature of labor and human capital in which each economic agent typically only holds one job, but instead mimics how workers can switch among jobs in the emergent on-demand economy. Second, as explained shortly, the production function of the mining industry represents an arms race, featuring a negative externality that each individual's acquiring more computation power directly hurts others' payoff. These two institutional features are key to understanding our results.

We first demonstrate the significant risk-diversification benefit offered by mining pools: under reasonable parameters, the certainty equivalent of joining a pool more than doubles that from solo mining. While this may lead to a hasty conclusion that a large pool would get ever larger, we show that in a frictionless benchmark with risk averse agents, full risk-sharing obtains but the pool size distribution is irrelevant. The risk-sharing benefit *within* a large pool could be alternatively obtained through miner diversification *across* multiple small pools — a general insight reminiscent of the Modigliani-Miller Theorem: Although investors (miners) are risk-averse, there is no reason for firms (pools) to form conglomerate for risk diversification purpose, simply because investors (miners) can diversify by themselves in the financial market by holding a diversified portfolio (joining different pools). In other words, the logic that pools merge for better risk-sharing when miners can freely allocate their hash

rates is simply unfounded.

Building on the benchmark insights, we introduce an empirically relevant friction: there are some "passive miners," however small, who do not optimally adjust their hash rate allocation in real time; they can be interpreted as those inattentive miners or potentially owners. Doing so allows us to incorporate pool heterogeneity and potential market power in the industry, in order to better understand the industrial organization of mining pools observed in practice and its impact on the mining arms race.

We fully characterize the equilibrium in this static setting, and find that the initial pool size distribution matters for welfare and future evolution of the industry. A large incumbent pool optimally charges a high 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: larger pools have a larger impact on the global hash power. In traditional industrial organization models, a bigger oligopolistic firm essentially charge higher prices and produces less. A similar effects manifests in our setting: larger pools charge higher fees to have proportionally less active mining, attracting less global hash power. Consequently, absent other considerations, we should expect an oligopoly market structure of the global mining industry to sustain in the long run, and no single pool grows too large to monopolize mining.

Instead of over-concentration, the real threat for the system's sustainability is that mining pools exacerbate the arms race which can be a huge social waste to the extent that the energy cost outweighs the enhanced security associated with blockchain systems. The global hash rates under full-risk-sharing is significantly higher than that under solo mining. Even though in equilibrium pool owners internalize the negative mining externality to some extent, quantitatively mining pools as a financial innovation still contributes significantly to the excessive energy consumption in cryptocurrency mining. In the case of Bitcoin, the existence of mining pools still easily multiply the global hash rates by 5-10 times of that under solo mining.

Empirical evidence from Bitcoin mining supports our theoretical predictions. First of all, though we do not claim causality, the rise of mining pools indeed coincides with the explosion of global hash rates and energy consumption on mining. Second, we provide cross-section evidence on pool size, pool fees, and pool growth. 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 show that pools with larger start-of-quarter size charge higher fees, and grow slower in percentage terms. We investigate these relationship in three two-years spans (i.e., 2012-2013, 2014-2015, and 2016-2017), and find almost of them are statistically significant with the signs predicted by our theory.

We further discuss the survival of market powers for pool managers with passive hash rates even with free entry, robustness of our results to aggregate risk modeling, and how the insights on risk-sharing and competition apply to alternative proof-of-work- or proof-of-stake-based blockchain protocols. We also discuss how other external forces counteract over-concentration of pools as well and could be added to our framework. Appendix C contains the analysis of short-term outcomes when the miners' hash rates are fixed.

More generally, our theory offers two novel economic insights: First, even though risk-sharing considerations leads to the formation of firms and conglomerates, it is not necessarily accompanied by over-centralization or concentration of market power. Second, what we really should worry about is that when agents or firms are engaged in an arms race with one's productions exerting negative externalities on others as seen in the cryptocurrency mining industry, a financial innovation or vehicle (mining pools that benefit individuals through risk-sharing) can be detrimental to welfare because it aggravates the arms race (excessive aggregate investment in hash power which can be socially wasteful), akin in spirit to Hirshlelfer (1971) and more recently Mian and Sufi (2015).

Related literature. Our paper contributes to emerging studies on blockchains and distributed ledger systems. Harvey (2016) briefly surveys the mechanics and applications of crypto-finance. Cong and He (2018) examine informational tradeoffs in decentralized consensus generation and how they affect business competition. Easley, O'Hara, and Basu (2017) and Huberman, Leshno, and Moallemi (2017) analyze the rise of transaction fees and the Bitcoin blockchain design. Several papers study the impact of blockchains on corporate governance (Yermack, 2017), holding transparency in marketplaces (Malinova and Park, 2016), financial settlements (Khapko and Zoican, 2017), 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).

Specifically, our study directly relates to cryptocurrency mining games. Nakamoto (2008) outlines the Bitcoin mining protocol as a well-functioning incentive scheme under adequate

decentralization. Biais, Bisiere, Bouvard, and Casamatta (2018) extend the discussion in Kroll, Davey, and Felten (2013) to model mining as coordination games and analyze equilibrium multiplicity. Kiayias, Koutsoupias, Kyropoulou, and Tselekounis (2016) consider a similar problem with explicit specification of states as trees. Dimitri (2017) and Ma, Gans, and Tourky (2018) model mining as Cournot-type competition and R&D race. Prat and Walter (2018) analyze the relationship between Bitcoin price and hash rate investment.

An adequate level of decentralization is crucial for the security of a blockchain. 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).[5] Eyal and Sirer (2014) and Eyal (2015) study "selfish mining" and miner's dilemma in which miners launch block-withholding attacks.[6] These papers follow the convention in the computer science literature to only consider one strategic pool behaving as a single decision maker.[7] In contrast, we characterize the full equilibrium wherein both miners and pools are strategic, in addition to modeling the incentives of participants and managers within each pool.

All the papers above on mining games 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. Our findings on the creation and distribution of mining pools also connect with strands of literature on contracting and the theory of the firm.[8] A few papers study contract design in mining pools, typically with one single pool (Rosenfeld, 2011; Schrijvers, Bonneau, Boneh, and Roughgarden, 2016; Fisch, Pass, and Shelat, 2017). We focus on the contracting relationships among miners and pool managers and the interaction of multiple pools in an industrial organization framework.

Importantly, although many blogs, think tank reports, and media article have taken notice of the large energy consumption by cryptocurrency mining, they focus on Bitcoin price and the type of processing chips (ASICs versus GPUs, e.g., Kugler (2018)), none has

[5] 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.

[6] 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.

[7] Beccuti, Jaag, et al. (2017) is an exception focusing on how miner number and heterogeneity affect block-withholding.

[8] Classical studies include Wilson (1968) on syndicates and Stiglitz (1974) on sharecropping. Recent studies include Li (2015) and Li (2017) on private information coordination.

modeled the mining industry and talked about the impact from mining pools, which we show to be of first-order importance in multiplying the energy usage.

The rest of the paper proceeds as follows. Section 2 introduces the institutional details of Bitcoin mining and stylized facts about mining pools. Section 3 sets up the model and discusses the frictionless benchmark, before Section 4 fully characterizes the equilibrium. 5 provides corroborating empirical evidence using Bitcoin data. Section 6 discusses model implications and extensions such as pool entry and alternative consensus protocols. 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.

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.[9] In order to win the competition, miners have to find a piece of data (known as solution), 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 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. Specifically, given a unit hash cost c and a dollar award R for

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

each block, the payoff to the miner who has a hash rate of λ_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 number of blocks the miner finds within T — a Poisson distributed random variable captures the risk that a miner faces in this mining game. Λ 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.

Note that this dynamic adjustment to the mining difficulty over time depends on the global hash power devoted to mining (an individual's success rate is scaled by the global hash rates Λ in Eq.(1)), and constitutes the driving force for the mining arms race.

The hash cost c is closely related to the energy used by computers to find the mining solution.

Because mining is highly risky, miners have strong incentives to find ways to reduce risk.[10] While theoretically there are various ways to reduce risk, a common practice is to have miners mutually insure each other by creating 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.[11] Ignore fees that represent transfers among pool members for now. Then, following the previous example, the payoff to one participating miner with hash rate λ_A who joins a pool with existing hash rate Λ_B (throughout we

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

[11] Note that because the space of candidate partial solutions is astronomical that 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.

use upper case Λ_m to indicate hash rates at the pool level) is

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

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. This is just the standard risk diversification benefit. We have the following proposition.

Proposition 1. *X_{pool} second-order stochastically dominates X_{solo}, so any risk-averse miner strictly prefers X_{pool} over X_{solo}.*

Hence pooled mining provides a more stable cashflow and reduces the risk a miner faces.

2.3 Quantifying Risk-Sharing Benefits of Pooled Mining

The risk-sharing benefit 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, i.e., exponential utility:

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

The resulting magnitude is be more or less robust to this utility specification, as we calibrate the risk-aversion parameter ρ based on the widely-accepted magnitude of the Relative Risk-Aversion coefficient.

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

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

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

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

We highlight that this certainty equivalent depends on the pool size λ_B and typically a larger pool offers greater risk diversification benefit.

We choose some reasonable numbers to gauge the magnitude of risk-sharing benefit of joining the 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 $CE_{solo} = 4.00216$ and $CE_{pool} = 9.25710$, which implies a difference of 5.25494, about 57% of the expected reward $\mathbb{E}(\tilde{X}_{solo})$ (about 9.25714). In other words, for a small miner, joining a large pool almost boost his risk-adjusted payoff by more than 131%.[12] 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 profit.[13]

There are two main implications for this diversification benefit. First, individual active miners who benefit from the risk-diversification acquire hash rates more aggressively to engage in the mining arms race; this potentially explains to the first order the large egregious energy consumption associated with cryptocurrency mining. Second, mining pools charge fees (price), which determine the individual miners' optimal hash rates allocation (quantity). The equilibrium fees, which should be lower than the monopolist fees calculated above due to competition among mining pools, depend on the industrial organization of mining pools. Note that even for well-diversified agents who can engage in infinitesimal mining over a long time, the benefit of diversification of idiosyncratic risk remains significant (Section 6.2 provides more details).

Before we develop a model to study these questions, we describe the various forms of fee contracts that in practice individual miners accept when joining a mining pool.

[12] Even if we set $\rho = .00001$ which implies 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%. And even for small pools, the risk-sharing benefit can be still quantitatively large. 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.

[13] 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 (or $c = \$3.96/(3600 \times 24 \times 13.5)$ per TH with \$3.96 daily power cost). 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.

2.4 Fee Contracts in Mining Pools

Pools in practice offer fee structures to its participating miners that could be categorized into three classes: *Proportional*, *Pay per Share* (PPS), and *Cloud Mining*. Table 3 gives the full list of contracts currently used by major pools, with Appendix B offering a full description of different reward types.

We next discuss these classes of compensation fee structure based on the contracting variables and the mapping from the contracting variables to payoffs. Technical details are left out unless they are necessary for understanding the unique feature of contracting in mining pools.

Pool managers and mining reward. A mining pool is often maintained by a pool manager, who takes a cut from miners' rewards at payout, known as pool fees which differ across pool contracts. In practice, all miners are subject to the same pool fee when contributing to the same pool under the same contract, independent of the level of their hash rates contributed to the pool. In other words, there is no observed price discrimination in terms of the pool fee charged.

Furthermore, different pools also vary in how they distribute transaction fees in a block. These transaction fees are different from "compensation/fees" that our model is analyzing; as discussed in Section 2.1, the transaction fees are what bitcoin users pay for including their transactions currently in mempool (but not on the chain yet) into the newly mined block. While most pools keep transaction fees and only distribute the coin reward from newly created block, given the rise of transaction fees recently more pools now also share transactions fees. Our reduced form block reward R encompasses both types of reward.

Effectively observable hash rates. All classes of fee contracts effectively use a miner's hash rate as 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 the so-called *partial solutions*. A partial solution to the cryptographic puzzle, like solution itself, is a piece of data such that the hash of all information about the block has at least an adequate number of leading zeros that is smaller than the one required by full solution. A solution, which can be viewed as "the successful trial," is hence always a partial solution. Counting the number of partial solutions amounts to measuring

the hash rates. Different observed contracts may use and weigh different partial solutions that represent different approximation methods, which are all proven to be quite accurate.

Crucially, the approximation error between the measured hash rate and the true hash rate can be set to be arbitrarily small with little cost. 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 diversification – a situation in stark contrast to that in Holmström (1982).

Fee contracts. As mentioned, the more than 10 types of fee contracts fall into three classes: proportional, pay per share (PPS), and cloud mining. These contracts differ in how they map each miner's hash rates to his final reward.

One predominant class entails proportional-fee contracts.[14] Under this contract, each pool participant only gets paid when the pool finds a solution. The pool manager charges a fraction f 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 hashrate λ_A joining a pool with an existing hashrate λ_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 class 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

[14] In practice, the most salient proportional contract is Pay-Per-Last-N-Shares (PPLNS), which instead of looking at the number of shares in a given round, looks at the last N shares regardless of round boundaries.

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 says 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 economic force can be easily adapted to the case of hybrid of proportional and PPS fees. There are two reasons for this modeling choice. First, in practice, about 70% of pools are adopting proportional fees, and 28% pools are using proportional fees exclusively.

The second reason is more conceptually important. Notice that the pure form of PPS or cloud mining is about risk allocation between miners and pool manager. Under our framework with homogeneous risk aversion among miners and pool managers, there is no welfare gain by adopting PPS or cloud mining. In contrast, a proportional fee contract enables risk sharing.

2.5 Stylized Facts about Mining Pools

Table 1 serves as a summary of the institutional background of the mining pool 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, measured by C5 which is the total market size of the top-5 pools sorted by hash rates) have mostly been increasing since 2011. As a gauge of overall cost in joining mining pools, Column D gives the average pool fee (including proportional, PPS, and others) weighted by hash rates for each year. 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 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 falls 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.[15]

[15]The proportional fees are in general smaller than "average fee" which is the average of proportional fees, PPS fees, and others. The reason is simple, and let us take PPS fees as an example. As explained, PPS contracts offer zero risk exposure to participating miners, and 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

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 hashrates contributed by top-5 pools (i.e., sum of the top five pools hash-rate over the market total hashrate, including those from solo-miners). In Column D, we report the average fee weighted by hashrates 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	Hashrate (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

3 An Equilibrium Model of Mining Pools

We present an equilibrium model where multiple pool managers compete in fees to attract customer miners. We first give a benchmark result: in a frictionless environment where all miners can actively determine their hash-rate acquisition and allocations to different pools, risk-sharing itself does not lead to centralization simply because miners can diversify themselves across pools. However, risk-sharing leads to a dramatic increase in global hash rate and thus a significantly more aggressive arms race.

Pool size distribution starts to matter in an interesting way when we assume that larger pools also have more passive miners who do not adjust their allocations. We show that larger pools charge higher fees, leading to slower pool growth. We then confirm key theoretical predictions using data on Bitcoin mining pools.

bearing more risk).

More importantly, no matter how the distribution of pool size evolves, mining pools as a form of financial innovation for risk sharing multiples the global hash power devoted to mining by several orders of magnitudes. To the extent that the blockchain consensus security does not improve linearly in the global hash power once it is above a certain threshold (which it does not in the case of the Bitcoin blockchain), this represents a tremendous waste of energy and detriment to the environment.

3.1 Setting

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

Pool Managers 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 Λ_{pm} (p stands for passive mining) existing hash rates from passive miners who stick to these pools. Empirically, we link Λ_{pm} to the pool size, under the assumption that a fixed fraction of miners do not adjust the hash rate contribution across pools. Passive hash rates include those from miners who do not pay attention to changes in pool sizes or fees at all times, the pool manager who commits to her own pool, or miners who derive special utility from a particular pool (e.g. strategic investors supporting the pool manager). Importantly, the measure of passive miners $\sum_m \Lambda_{pm}$ matters little for our qualitative results.[16]

Thanks to the significant risk sharing benefit to individual miners explained in Section 2, managers of pools $\{m\}_{m=1}^M$ post (proportional) fees $\{f_m\}_{m=1}^M$ simultaneously to maximize profits, where the fee vector $\{f_m\}_{m=1}^M$ is determined in equilibrium.

Active miners' problem There is a continuum of active homogeneous miners of total measure N, each of whom can acquire hash power with a constant unit cost c. In other words, active miners are competitive while mining pools may enjoy market power. In Appendix C, we discuss the case where active miners are endowed with fixed hash rates, and show our conclusions concerning the industrial organization of mining pools remain robust.

[16]This modeling assumption that only a fraction of players can actively readjust 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)). In the practice of Bitcoin, although it involves almost no cost of switching, inattention suffice to generate inertia in switching among pools. Our model predictions do not depend on the exact mechanisms of passive miners.

Taking the fee vector $\{f_m\}_{m=1}^M$ as given, these active miners can acquire and allocate their hash rates to the above m pools. Optimal allocation among existing pools, rather than a binary decision of participation, plays a key role in our analysis. Here, we also implicitly assume that these infinitesimal active miners lack the expertise to become the pool managers (they are just customers of mining pools). This is consistent with the fact that most individual miners simply use mining softwares and setting up a mining pool is an elaborate process; or they lack the commitment device of locking their hash rates.

Consider an active miner who faces $\{\Lambda_{pm}\}_{m=1}^M$ and $\{f_m\}_{m=1}^M$. The payout when allocating a hash rate of λ_m to pool m is

$$X_m = \frac{\lambda_m}{\Lambda_{am} + \Lambda_{pm}} \tilde{B}_m (1 - f_m) R, \tag{8}$$

where Λ_{am} (a stands for active mining) is the hash rate contribution to pool m from all active miners. Recall that throughout we use lower case λ to indicate individual miner's decisions while upper case Λ_m for hash rates the pool level.

We use $m = 0$ to indicate solo mining, in which case $f_0 = \Lambda_{pm} = 0$. As a result, the active miner with exponential utility function $u(x) = \frac{1}{\rho}\left(1 - e^{-\rho x}\right)$ chooses $\{\lambda_m\}_{m=1}^M$ to maximize

$$\mathbb{E}\left[u\left(\sum_{m=0}^{M} X_m - C\sum_{m=0}^{M}\lambda_m\right)\right] \;=\; \mathbb{E}\left[u\left(\sum_{m=0}^{M}\left(\frac{\lambda_m \tilde{B}_m(1-f_m)}{\Lambda_{am}+\Lambda_{pm}}\right)R - C\sum_{m=0}^{M}\lambda_m\right)\right].$$

Here, we we denote cT as C. Since our analysis works under any choice of T, for brevity of notation we further normalize $T/D = 1$. Then certainty equivalent calculation implies that the hash contribution problem to each pool decouples from one another, and the optimization is equivalent to

$$\max_{\lambda_m \geq 0}\left[\frac{\Lambda_{am}+\Lambda_{pm}}{\rho\Lambda}\left(1 - e^{-\frac{\rho R(1-f_m)\lambda_m}{\Lambda_{am}+\Lambda_{pm}}}\right) - C\lambda_m\right], \forall m, \tag{9}$$

where the global hash rate Λ is

$$\Lambda = \sum_{m=0}^{M}(\Lambda_{am} + \Lambda_{pm}). \tag{10}$$

In (9), the global hash rate Λ 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 to understand our results later.

We impose two parametric assumptions, which significantly simplies our derivation and are also supported by empirical data.

Assumption 1. $\rho R < N$.

In our model, when facing a higher proportional fee, an active miner weighs two opposite effects: the first-order effect of a lower expected reward that expels the miner, and the second order effect of a lower risk that attracts the miner. This assumption holds under realistic parameters and requires the risk aversion to be adequately small to guarantee that the first-order effect dominates.

Assumption 2. $\rho C \left(\sum_m \Lambda_{pm} + \frac{R}{C} e^{-\rho R/N}\right) > 1 - e^{-\rho R}$.

The assumption requires that the sum of passive mining and the active mining in the absence of passive mining (which we later calculate to be $\frac{R}{C} e^{-\rho R/N}$ in Proposition 1) is relatively large that solo-mining is not profitable given the difficulty level of mining. Solo-mining is not our economic mechanism and ruling it out allows us to greatly simplify the exposition.

Pool manager's problem. A pool manager with passive hash rate Λ_{pm} sets a proportional fee f_m to maximize her expected utility.[17].and Λ_{am} is the hash rate that the pool m is able to attract from active miners, which depends on the fee charged.

[17]In practice, a significant portion of Λ_{pm} may belong to the pool manager himself, and we can easily incorporate this case in our model by replacing f_m in (12) with $\hat{f}_m$, so that

$$\hat{f}_m = \frac{\Lambda_{am}}{\Lambda_{am} + \Lambda_{pm}} f_m + \frac{\Lambda_{pm}}{\Lambda_{am} + \Lambda_{pm}} \alpha(f_m), \tag{11}$$

where $\alpha(f) \in [f, 1]$ is weakly increasing in f. One useful way to understand this function is the following: Suppose the manager owns a fraction π of the passive mining power, while the rest $1 - \pi$ comes from other fee-paying loyal passive miners. For example, as revealed in an interview between Bitcoin Magazine and the CEO of the large mining pool ViaBTC, "(ViaBTC) had an investor at its early stage who provided us with the startup capital and hash rate, but didn't take part in the decision-making and operating of the mining pool", and "approximately one third of the hash rate is from our investor, and the rest from our customers." Then $\alpha(f) = \pi + (1 - \pi)f$ is increasing in f, which is a special case of a monotone $\alpha(f)$. For exposition ease, in the main text we set $\alpha(f) = f$ and hence $\hat{f}_m = f_m$, although in an earlier draft we show that all the proofs go through with the more general formulation of $\hat{f}_m$ given in Equation (11)

We study the fee-setting game among pools. Given $\{\Lambda_{pm}\}_{m=1}^{M}$ and the fee charged by other pools f_{-m}, the m-pool manager chooses f_m to maximize

$$\max_{f_m} \frac{\Lambda_{am}(f_m) + \Lambda_{pm}}{\rho\Lambda(f_m, f_{-m})} \left(1 - e^{-\rho R f_m}\right). \tag{12}$$

It is worth emphasizing that when pool managers choose their fees, these oligopolistic pools understand that the global hash power Λ depends on the fees charged by pool m and other pools $(-m)$, because pool fees affect pools sizes which in turn affects the global hash power. In other words, pool owners partially internalize the arms-race externality.

3.2 Definition of Equilibrium

Consider the class of symmetric subgame perfect equilibria where homogeneous active miners take the same strategies. The notion of "subgame" comes from that active miners are reacting to the fees posted by M pool manage paths. In other words, any pool is facing an aggregate demand function as a function of the fee vector, and all homogeneous active miners are taking symmetric best responses to any potential off-equilibrium fee quotes.

Equilibrium Definition Consider the class of symmetric subgame perfect equilibria where homogeneous active miners take the same strategies. An equilibrium is a collection of $\{f_m, \lambda_m\}_{m=1}^{M}$ so that

(1) **Optimal fees:** Given $\{f_{-m}\}$ set by other pool managers, f_m solves pool manager m's problem in (12) for all $m \in \{1, 2, \cdots, M\}$;

(2) **Optimal hash rates allocation:** Given $\{f_m\}_{m=1}^{M}$, $\{\lambda_m\}_{m=1}^{M}$ solves every active miner's problem in (9);

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

3.3 The Frictionless Benchmark

The initial size distribution of mining pools matters because we assume it is proportional to the measure of passive miners $\{\Lambda_{pm}\}_{m=1}^{M}$. To highlight the role of passive miners in our model, we first analyze the model outcome absent passive miners as a benchmark.

Irrelevance of pool distribution for risk sharing. We first present a stark irrelevance result of pool size distribution for risk-sharing in the frictionless case without passive mining.

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

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

(2) Symmetric miners set any allocation $\{\lambda_m\}_{m=1}^M$*, as long as the global hash rates* Λ *satisfies*

$$\Lambda = N \sum_{m=1}^{M} \lambda_m = \frac{R}{C} e^{-\rho R/N}. \tag{13}$$

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

In this class of equilibria, the global hash power that miners acquire is $\Lambda = \frac{R}{C} e^{-\rho R/N}$, so that for each miner the marginal benefit of acquiring additional hash power hits the constant acquisition cost C. Under zero fees, each individual miner is maximizing his objective in (9); and Assumption 2 rules out solo-mining. Fixing the total hash power Λ in this economy, the allocation among pools reaches efficient risk-sharing among all miners. Pool managers charge zero fees for a Bertrand type argument: otherwise one pool manager can cut her fee to steal the entire market because they offer identical services. We will see later that the key friction $\Lambda_{pm} > 0$ renders some market powers to pools, leading to a monopolistic competition in this economy.

Fallacy of risk diversification and pools. Numerous discussions in the cryptocurrency mining community have focused on the centralization implications of risk diversification, i.e., joining larger pools is attractive and would lead to even more hash rates joining the largest pools, making larger pools even more concentrated. Proposition 1 dispels the myth and reveals a Modigliani-Miller insight: In a frictionless market investors can perfectly diversify by themselves, rendering no rationale for conglomerates to exist solely for risk sharing. In other words, as long as miners can join the pools in a frictionless way, there is no reason to expect that a single large pool necessarily emerges (say, via mergers).

In practice, switching between pools involves simply changing one parameter in the mining script and hence participating in multiple pools entails negligible transaction cost.[18] As

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

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 becomes futile for risk-sharing purposes.

Proposition 1 also implies that from the perspective of individual miners, there is no risk-diversification benefit for pools to merge into a conglomerate—individuals miners can simply diversify across pools. This insight applies throughout this paper, even in later analysis with friction where pools are endowed with passive rates Λ_{pm}. There, pool managers might have motives to merge for a greater market power, but this force is distinct from risk-diversification and is be counter-balanced by potential entry (see Section 6.1).

Arms race effect and the dark side of mining pools. Proposition 1 also reveals another equally important point: Although the class of equilibria features full risk-diversification, it does not feature the first-best outcome in our model. Due to the nature of arms race, the equilibrium global hash rates $\Lambda = \frac{R}{C}e^{-\rho R/N}$ are excessive; within our model, the first-best investment in computational power has the entire system spend ϵ amount of hash rates to generate the same reward R.

Moreover, under solo-mining, the equilibrium global hash rates $\Lambda = \frac{R}{C}e^{-\rho R}$. In contrast, the global hash rates under mining pools are significantly higher because risk-sharing effectively increases the risk tolerance by a factor of N. This aggravation of arms race costs huge amount of additional energy and can be environmentally damaging. We further elaborate these points in the next section once we fully characterize the equilibrium.

4 Equilibrium Characterization and Implications

Now we allow the passive mining friction Λ_{pm}, and characterize the equilibrium quantity and distribution of mining activities. Λ_{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.

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 standard portfolio allocation problem in financial investment. In contrast, it is much harder for workers to hold multiple jobs.

4.1 Fees and Active Miners' Allocation

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 (9) gives,

$$\underbrace{\frac{R(1-f_m)}{\Lambda}}_{\text{risk-neutral valuation}} \underbrace{e^{-\rho R(1-f_m)\frac{\lambda_m}{\Lambda_{am}+\Lambda_{pm}}}}_{\text{risk aversion discount}} = \underbrace{C}_{\text{marginal cost}} . \tag{14}$$

The left (right) hand side gives the marginal benefit (cost) of when allocating λ_m to a pool with size $\Lambda_m = \Lambda_{am} + \Lambda_{pm}$. For the marginal benefit, the first term is the risk-neutral valuation of the marginal benefit per unit of hash power; it is R times the probability of winning ($\frac{1}{\Lambda}$) given global hash rates Λ, adjusted by proportional fee. The second term captures the miner's risk-aversion discount. Conditional on his allocation λ_m, the larger the pool size Λ_m he participates, the smaller the discount–this is exactly illustrated by Section 2.3. But conditional on the pool size, the risk-aversion discount worsens with his allocation λ_m. The optimal allocation rule equates marginal benefit with marginal cost, and the greater diversification benefit of larger pools leads to more participation of active miners (in an absolute sense).

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

$$\frac{\lambda_m}{\Lambda_{pm}} = \max\left\{0, \frac{\ln\frac{R(1-f_m)}{C\Lambda}}{\rho R(1-f_m) - N\ln\frac{R(1-f_m)}{C\Lambda}}\right\}, \tag{15}$$

where zero captures the corner solution of a pool not getting any active miner (e.g., when f_m is high enough). Equation (15) directly leads to the following proposition characterizing how pool fees relate to equilibrium active mining in each pool.

Proposition 2 (Active Mining)**.** *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 $\frac{\lambda_m}{\Lambda_m} < \frac{\lambda_{m'}}{\Lambda_{m'}}$.*

If pools are charging the same fee, then larger pools with greater diversification benefit attract more active miners, so much so that each pool grows with the same proportion. In

a similar vein, pools that charge higher fees have a slower growth, cross-sectionally.

4.2 Pool Managers' Fee-setting

Now for pool owners, the objective in (12) can be written as

$$\frac{\Lambda_{am}(f_m)+\Lambda_{pm}}{\Lambda(f_m,f_{-m})}\left(1-e^{-\rho R f_m}\right)=\frac{\Lambda_{am}(f_m)+\Lambda_{pm}}{\Lambda_{am}(f_m)+\Lambda_{pm}+\Lambda_{-m}}\left(1-e^{-\rho R f_m}\right) \tag{16}$$

where $\Lambda_{-m}=\sum_{m'\neq m}\left(\Lambda_{am'}+\Lambda_{pm'}\right)$ is the global hash power lest pool m's. Relative to the miner's problem in (9), pool owners engage in oligopolistic competition, and take into consideration that f_m not only affects their pools' hash rate but also the global hash rate. We plug Eq. (15) into Eq. (16), while clearly indicate the dependence of global hash rate on pool fees, to obtain

$$\underbrace{\frac{1-e^{-\rho R f_m}}{\Lambda(f_m)}\cdot\max\left\{1,\frac{\rho R(1-f_m)}{\rho R(1-f_m)-N\ln\frac{R(1-f_m)}{C\Lambda(f_m)}}\right\}}_{\text{value per unit of initial size }\Lambda_{pm}}\cdot\underbrace{\Lambda_{pm}}_{\text{initial size}} \tag{17}$$

In Eq.(17), each pool manager not only set fees to maximize her value per unit of her initial size, but also takes into account the impact of her fee setting on the global hash rates $\Lambda(f_m)$ through the arms race effect.

4.3 Symmetric M-pool Equilibrium

When all pools are with the same hash rates $\Lambda_{mp}=\Lambda_p$ for all m, the equilibrium outcome is characterized by two endogenous variables: the fee charged by each pool, and the global hash rates in all the pools. The next proposition characterizes the equilibrium in one nonlinear equation, by combining (15) and the first-order condition of (17).

Proposition 3. *Consider the case where pools are symmetric with identical passive hash rates $\Lambda_{pm}=\Lambda_p$ for all m, and focus on the case where the equilibrium fee admits an interior solution. Let $z(f)\equiv\frac{(m-1)\left(1-e^{-\rho R f}\right)[N-\rho R(1-f)]}{me^{-\rho R f}\rho^2R^2(1-f)-(m-1)\left(1-e^{-\rho R f}\right)}$. Then in equilibrium the global hash rates $\Lambda=\frac{m\Lambda_p}{z(f)}$, where the equilibrium fee f solves*

$$\rho R\left(1-f\right)\left(1-z\left(f\right)\right)=N\ln\frac{R\left(1-f\right)z\left(f\right)}{mC\Lambda_p}.$$

We illustrate the equilibrium outcome in this symmetric-M pool economy, by highlighting the implication of mining pools as a financial innovation on the arms race.

4.4 Financial Innovation and Arms Race

With a good understanding of our benchmark and the symmetric-pool equilibrium, it is opportune to discuss how the emergence of the industry affect the mining arms race, before we move onto analyzing the industrial organization of mining pools.

As we have mentioned, the class of equilibria characterized by Proposition 1 do not feature the first-best outcome in our model. Without any passive hash rates, based on (9) the social welfare of any representative active miner can be calculated as:[19]

$$\frac{1}{\rho}\left(1-e^{-\frac{\rho R}{N}}\right)-C\Lambda. \tag{18}$$

This implies that the first-best allocation will have Λ to be as small as possible.

At the heart of this result is that the mining game is an arms race: acquiring an additional unit of hash rate raises the global hash power Λ, hence imposing negative externality on other miners by increasing the difficulty of the problem they are solving. And the increased difficulty does not produce any additional social surplus, as each representative active miner always gets the benefit of $\frac{1}{\rho}\left(1-e^{-\frac{\rho R}{N}}\right)$ from mining. As a result, the first-best benchmark allocation in our mining economy has miners acquire ϵ hash power each, receiving R with almost no cost, and then share the reward equally among all miners.

Recall that absent mining pools, 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, $\frac{R}{C}e^{-\rho R/N}$.[20] As a result, the aggregate miner surplus with mining pool is lower than that without—an example of financial innovation/vehicle that seemingly benefits individuals but in aggregate could lower welfare. And the welfare loss turns significant precisely when the risk-sharing benefit of mining pools is large–say, when the risk-aversion ρ is high, or the measure of active miners N is large.

[19] Proposition 1 shows that without Λ_{pm} we can without loss of generality to consider just a single pool without any fees; so in equilibrium $\lambda_m = \Lambda_{am} = \Lambda$

[20] Due to our continuum specification of miners, an infinitesimal miner would not solo-mine because of his infinitesimal risk tolerance. The way to get around this artifact of modeling choice is to view active miners as groups of unit measures, and then apply the same condition (14) in that marginally no active miner wants to acquire more solo hash rate.

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 will be lower in the main model with frictions, for two reasons: first, passive miners who do not diversify into various pools, and second, active miners are facing strictly positive fees set by pools. However, under reasonable parameter choices, the implied global hash rates with mining pools can still be more than five times that without mining pools.

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: 1) solo-mining without pools; 2) full risk-sharing implied by Proposition 1 without passive mining friction; and 3) oligopolistic competition with passive hash rates as initial pool size, with $m = 2$. Panels A and B plot the global hash rates Λ for two risk-aversion coefficients ρ; Panels C and D plot Λ for two values of the active miner measure N.

First of all, we observe that for solo-mining, the implied global hash rates increases with reward R initially but actually decreases when R is sufficiently large; this is because the risk becomes overwhelmed when R increases.[21] Second, when we compare Panel A (B) with C (D) which feature $N = 10$ and $N = 500$ respectively, they by definition have the same solo-mining outcomes, and their full risk-sharing hash rates differ by at most a factor of 1.3. This 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).

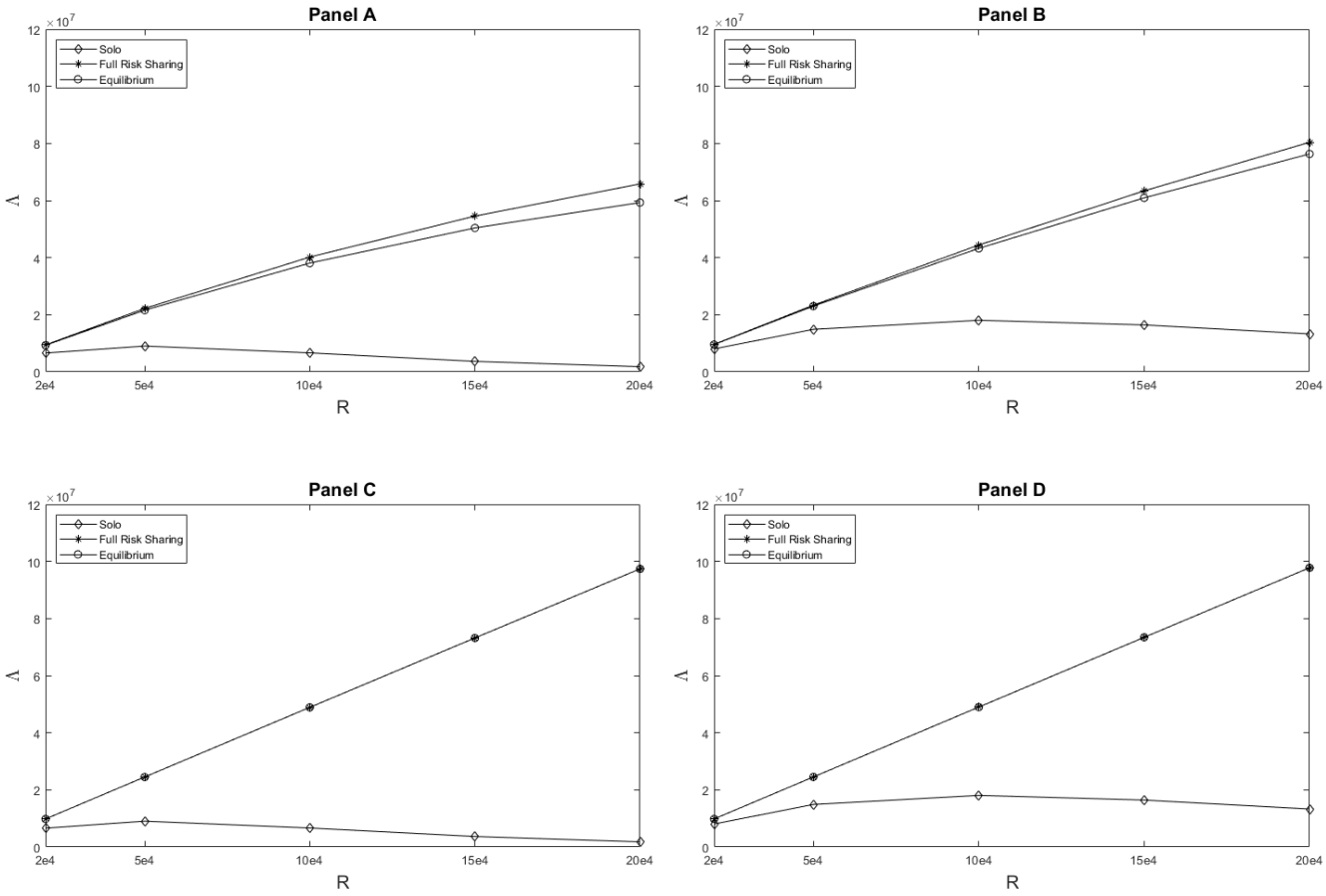
Now we move on to the equilibrium outcome under mining pools with passive hash rates. Relative to solo mining, both the full risk-sharing and the mining pool equilibrium produce about ten times of global hash rates for $\rho = 2 \times 10^{-5}$ and $R = 10^5$, for both levels of N. This wedge gets amplified 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 $40 \sim 50$ times of that with solo mining. The arms race escalates when miners are more risk-averse.

As expected, the symmetric two-pool equilibrium generates lower global hash rates compared to the full risk-sharing benefit. Intuitively, pool managers with some market power are take into account the arms race effect and hence discourage active miners' hash power acquisition by raising their fees. Although we have given the best chance of this market power force by setting the lowest possible of number of pools (here, $m = 2$), quantitatively

[21] This result depends on our CARA preference which has no wealth effect.

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

Global hash rates Λ is plotted against block reward R under various parameters. We consider symmetric M pools each with passive hash rates $\Lambda_p = 3 \times 10^5$. The common parameter is $C = 1.375 \times 0.12/(3600 \times 13.5) \times 600 = 0.00204$, 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: $M = 2, N = 500, \rho = 2 \times 10^{-5}$ Panel D: $M = 2, N = 500, \rho = 1 \times 10^{-5}$.



there is not that much of this countervailing effect. In fact, the difference between the full risk-sharing and two-pool cases becomes invisible N is large (Panel C and D). When there are more active miners to compete so N is large, pools are engaging in a more aggressively competition which is the root of arms race.

The take-away from Figure 2 is that the introduction of mining pools as a form of financial innovation exacerbates the arms race and is likely behind the egregious amount of energy consumed in cryptocurrency mining in recent years. It is important to mention that we are cognizant of the benefits of PoW protocols and the arms race nature of competition (Cong and He (2018) and Abadi and Brunnermeier (2018), among others), which are outside

our model. But at least for Bitcoin, the social benefit seems small compared to the energy consumption and environmental damage. First, the verifications on bitcoin blockchain are simple, presumably alternative designs can generate similar consensus at lower costs. Moreover, above certain threshold, the security benefit does not increase linearly with the hash power devoted to mining.

4.5 Heterogeneous Pools and Equilibrium Pool Growth.

Now we allow pool sizes to be heterogeneous and study the equilibrium growth.

Proposition 4 (Endogenous Pool Fees)**.** *For any two pools m and m', if $\Lambda_{pm} > \Lambda_{pm'}$, then $f_m \geq f_{m'}$ in equilibrium.*

The intuition of Proposition 4 is rooted in that pools with a larger initial size of passive miners would take into account its larger "global hash rate impact" (increase in mining difficulty) by changing their fees, akin to the standard "price impact" in any monopolistic setting. To see this, suppose pool owners ignore the fee impact on global hash rate, then $\Lambda(f_m)$ would be a given constant Λ, and the optimal choice of f_m will maximize the term "value per unit of Λ_{pm}" and thus completely separates from initial pool size Λ_{pm}. Consequently, pool owners all charge the same fee, and hence attract active mining in proportion to their initial size.

However, pool managers who behave as oligopolists in this economy 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 Λ and hurting her pool profits—exactly the arms race effect. Because every unit of active hash rate affects the aggregate hash rates equally, on the margin, larger pools who also take into account the "global hash rate impact" or the arms race nature of the game would have a stronger incentive to raise fees and curb the increase in mining difficulty. This mimics the standard oligopolistic setting in which firms with larger market power charging higher prices and produce relatively less.[22]

Combining Propositions (2) and (4), we arrive at our key conclusion concerning the distribution of pool sizes.

[22]Our results are not driven by the fact that pool managers benefit from charging a higher fee to get higher revenues from the passive miners, which is trivially larger when Λ_{pm} is greater. 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. Therefore, this consideration only affects equilibrium fees charged through its interaction with active mining and the "global hash rate impact."

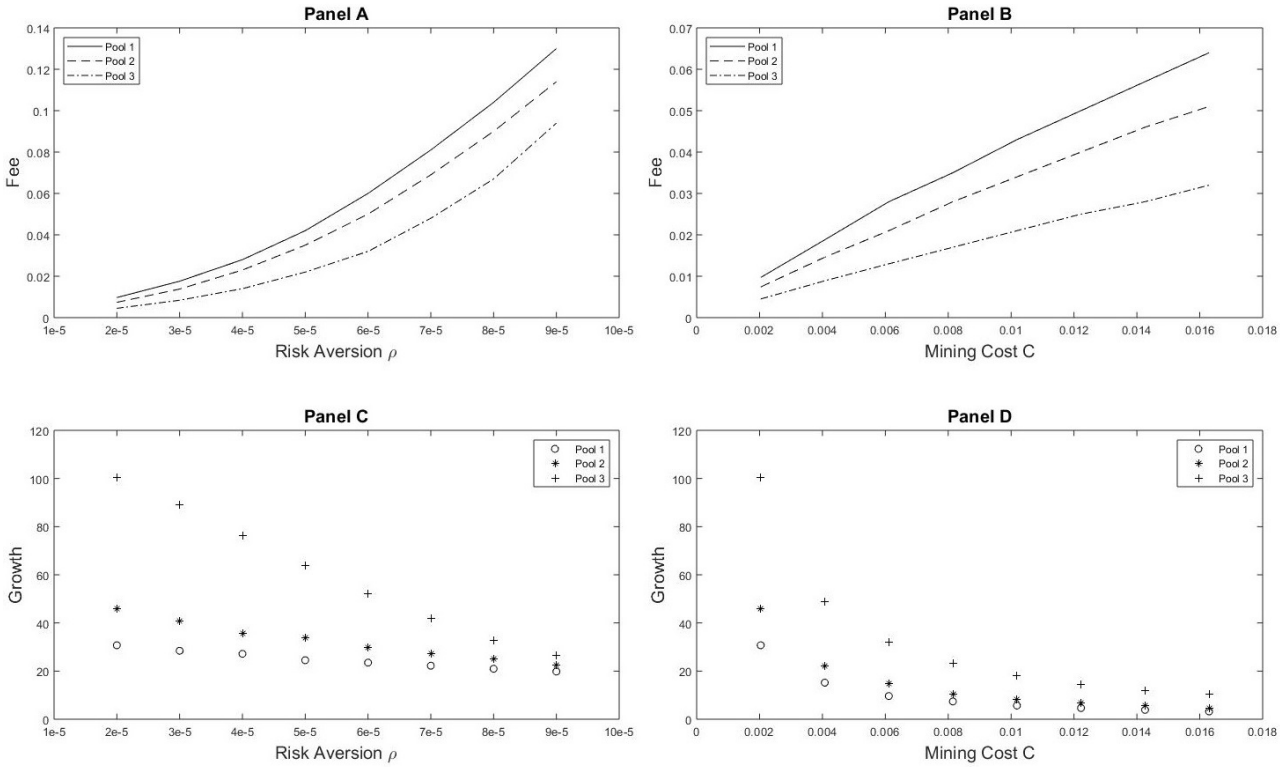
Corollary 1 (Pool Growth Rate)**.** *Pools with larger initial size* Λ_{pm} *have weakly smaller* $\frac{\Lambda_{am}}{\Lambda_{pm}}$*, leading to a weakly lower growth rate.*

This result implies that mining pools do not grow more concentrated. A natural force from the market power of larger pools combined with the arms race nature of mining technology limits their growth, allaying the concern that the rise of mining pools would lead to excessive centralization and instability of the consensus system.

For illustration, we investigate the properties of a three-pool equilibrium in Figure 3 by studying the comparative statics of the equilibrium objects: the endogenous fees charged by pool managers $\{f_1, f_2, f_3\}$, as well as equilibrium pool net growth $\{\Lambda_{a1}/\Lambda_{p1}, \Lambda_{a2}/\Lambda_{p2}, \Lambda_{a3}/\Lambda_{p3}\}$.

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

Equilibrium fees $\{f_1, f_2, f_3\}$ and the net growth rate of two pools $\Lambda_{a1}/\Lambda_{p1}, \Lambda_{a2}/\Lambda_{p2}$, and $\Lambda_{a3}/\Lambda_{p3}$ are plotted against miner risk aversion ρ and unit hash power cost C, respectively. The baseline parameters are: $R = 1 \times 10^5$, $\Lambda_{p1} = 5 \times 10^5, \Lambda_{p2} = 3 \times 10^5$, $\Lambda_{p3} = 1 \times 10^5$, and $N = 10$. In Panel A and C: $C = 1.375 \times 0.12/(3600 \times 13.5) \times 600 = 0.00204$. In Panel B and D: $\rho = 2 \times 10^{-5}$.



Without loss of generality, we set $\Lambda_{p1} > \Lambda_{p2} > \Lambda_{p3}$. Panel A presents how the equilibrium fees respond to exogenous changes in risk aversion ρ in this economy, and Panel B presents

how the equilibrium fees vary with the unit hash power acquisition cost C.

Not surprisingly, when the economic agents become more risk averse, individual miners' demand for risk-diversification increases, 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. Though not plotted in Figure 3, it is clear from Panel C that the endogenous global hashrates are decreasing in the risk aversion.

Panel B and D illustrate how the equilibrium outcomes change when we vary the constant hash power acquisition cost C. The lower the hash power acquisition cost, the more the active hash rates to compete for mining pools, and the lower the fee given greater competition. The cross-pool fees distribution and pool growth are similar to other panels.

Importantly, the absence of dominant pools over time implies that the market power and internalization of mining externality by pool owners is small relative to the extent risk-sharing through mining pools encourage individuals to acquire additional hash power. Consequently, the aggravation of the mining arms race is not mitigated much by the presence of heterogeneous mining pools (Figure 2).

5 Empirical Evidence

The theoretical analyses in previous sections offer three predictions. First, as the Bitcoin mining market becomes increasingly dominated by mining pools, the global hash rate increases significantly. This is apparent from Figure 1. Moreover, cross-sectionally, a pool with larger starting size tends to (i) charge a higher fee, and (ii) grow slower in percentage terms. In this short section we provide supporting evidence for these two predictions.

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, divide it 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

real-timeness and precision of estimation, we take the time interval to be weekly.[23]

In part two, the fee contract information 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.[24] Pool fees are aggregated to quarterly frequency by simple average.

The two parts are then merged to construct a comprehensive panel data on pool size and fee evolution. Our main analysis focuses on the evolution of pool sizes at the quarterly frequency given potentially lagged adjustment. Table 1 in Section 2 provides summary statistics of the data.

Empirical results. Since our model predictions concern about cross-sectional relationships, every quarter we first sort pools into deciles based on the start-of-quarter pool size (estimated hashrate share within the first week). We then treat each decile as one observation, and calculate the average proportional fee and average log growth rate across mining pools for each decile.

Figure 4 shows the scatter plots for these decile-quarter observations, with Panel A (B) being 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, Figure 4 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. Importantly, all regression coefficients are statistically significant at 5% level for all three time periods. The detailed regression results are reported in Table 2.

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-

[23] Our estimation procedure is standard. For example, blockchain.info provides real-time updates about estimated hashrate distribution over the past 24 hours, 48 hours, and 4 days using the same method. Bitcoinity tracks about 15 large mining pools' real time hashrate 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.

[24] 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.

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.

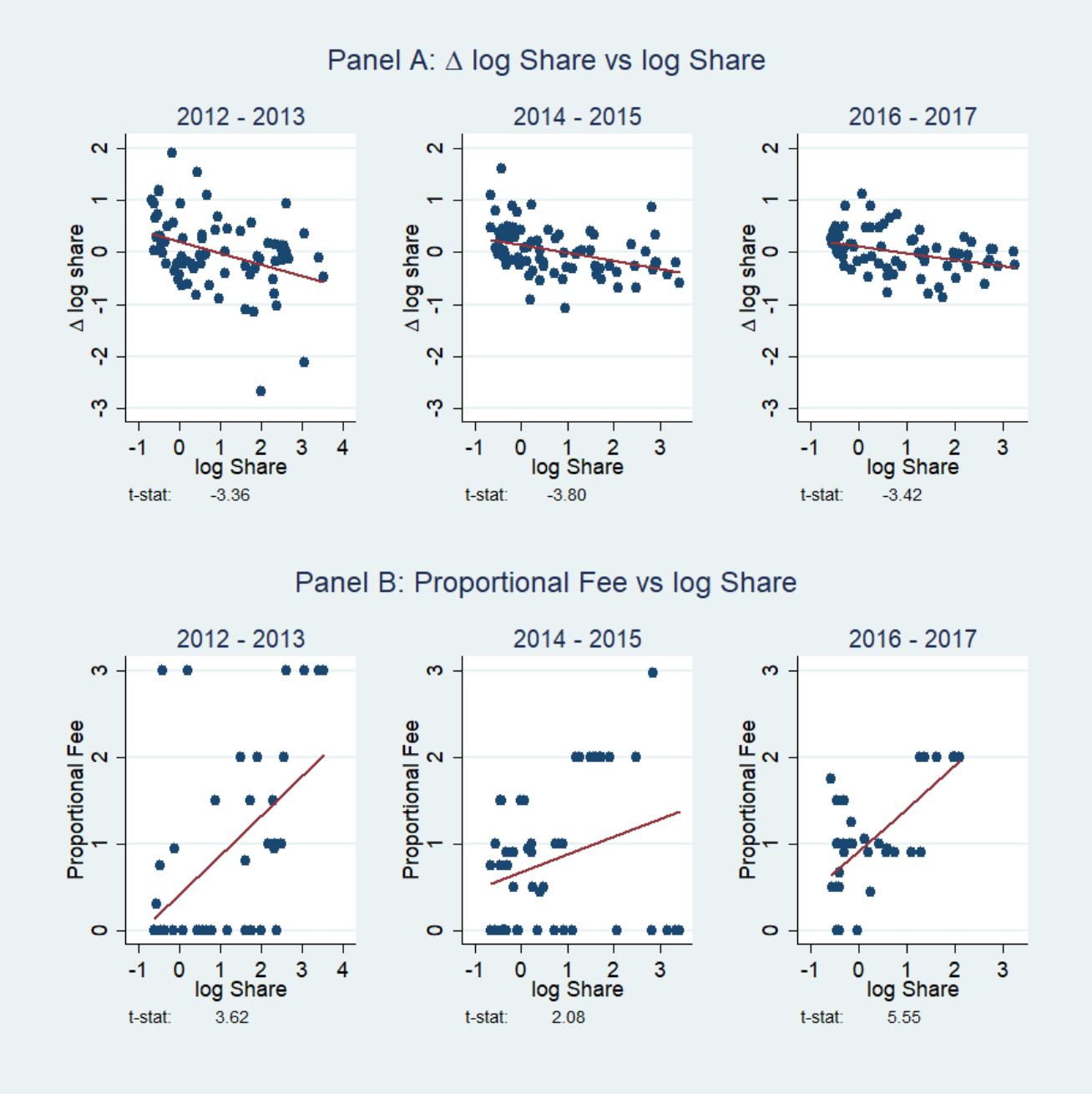


Table 2: **Pool Sizes, Fees, and Growths: Regression Results**

This table reports the regression results when we regress *Proportional Fee* and $\Delta logShare$ on $logShare$, respectively. Share is the quarterly beginning hashrate over total market hashrate. 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
$* : p < 0.05, ** : p < 0.01, *** : p < 0.001$

stake. Along the way, we also present an economist' perspective on several important issues such as the nature of risk and regarding 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. Since our economic mechanism borrows extensively from the literature of industrial organization, this section discusses the pool's intrinsic monopoly power thanks to its passive hash rates, and show that our key economic forces are robust to potential entry of competing mining pool managers.

We first consider the possibility of free entry of pool managers who do not have passive hash rates. Due to the nature of portfolio risk-diversification, incumbent pool managers with passive hash rates are facing a monopolistic competition, in which they are offering strictly

better products/services than the entry pool without. In fact, incumbent pool managers are as if with some monopolistic power, and in equilibrium always charge some strictly positive fees to some active miners. We then briefly discuss the potential entry of pool managers with passive rates, so that the number of pools is endogenously determined by the entry condition. Finally, even if there are infinite number of pools, the nature of monopolistic competition still survives with each pool making strictly positive profits.

Pool entry without passive hash rates. We denote the number of incumbent pools with passive hash power 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 managers, who are financially constrained entrepreneurs, do not have passive hash rates (e.g., they lack supporters loyal to their pools) 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 mining pools.

In our model, the entrant pools without passive hash rates may attract a positive measure of active miners as they may charge a low fee in equilibrium. But, the following proposition reveals that without loss of generality, at most one pool without passive hash rates enters, and incumbent pools always enjoy a certain amount of 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 power, even with free entry ($K = 0$).

The first part of the proposition follows from Proposition 1. Entrant pools are homogeneous and compete away any net profit among themselves. Therefore in equilibrium at most one pool enters and breaks even. Proposition 1 implies that when $K = 0$, the pool size distribution 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 λ_m

and Λ_{am} to zero in $R(1-f_m)e^{-\rho R(1-f_m)\frac{\lambda_m}{\Lambda_{am}+\Lambda_{pm}}}$ in Eq. (14), which gives

$$\frac{R(1-f_m)}{\Lambda}, \tag{19}$$

exactly the post-fee risk-neutral valuation.

Suppose, counter-factually, that all incumbent pools charge zero fee $f_m = 0$; then the risk-neutral valuation $\frac{R}{\Lambda}$ in Eq. (19) must exceed the marginal cost C and in any equilibrium with strictly positive active mining (due to the risk-aversion discount in Eq.(14)).[25] As a result, incumbent pools start charging positive fees, which inefficiently pushes more active hash rates toward the zero-fee entry pool relative to the optimal risk sharing benchmark (absent of fees).

Compared with a standard perfectly competitive market wherein a Bertrand-type price competition allows entry firms to compete away incumbents' profits, 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.

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

Pool entry with passive hash rates and number of incumbents. 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 that are not costless, the entry costs are strictly positive ($K > 0$). 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

[25] 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 $\frac{R}{\Lambda} > C$.

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 (including the acquisition cost of passive rates and set-up cost).

One thought-provoking question is, given the equilibrium entry of total passive hash rates, can we restore perfect competition by increasing the number of competing pools and at the same time shrink the pool size (e.g., splitting the pools)? In other words, would pools lose their monopolistic power when we have $M \to \infty$? The discussion about Eq.(14) suggests a negative result, as long as the size of active miner is infinitesimal relative to the size of mining pool.[26] In fact, if we have a continuum of pools who take the global hash rates Λ as given, then the same logic as in the discussion of Proposition 4 in Section 4 implies that all pool managers enjoy a positive market power and charge the same strictly positive fee as in Eq.(17) in the absence of the arms race effect.

6.2 The Nature of Risk

Given that risk-sharing drives the formation of mining pools, several questions regarding the nature of the risk arise. First, it is clear that 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 diversifying idiosyncratic risk (via pools), not the pricing of idiosyncratic risk. Idiosyncratic risk matters little for pricing exactly because agents diversify it out.

The idiosyncratic nature of mining risk may also prompt researchers to reach the hasty conclusion that 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, as 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, when miners acquire an infinitesimal amount of hash rate, it shrinks the probability of winning toward zero but does not shrink the magnitude of (risky) reward.[27] If this reward is significant

[26]For instance, in theory with financial intermediaries we often assume a continuum of banks and each bank serves a continuum of depositors.

[27]In standard asset pricing models, the agent with utility function u who is consuming $\widetilde{C}$ and facing an asset with idiosyncratic payoff $\widetilde{R}$ and price p, is solving $\max_\epsilon \mathbb{E}\left[u\left(\widetilde{C}+\epsilon\widetilde{R}-\epsilon p\right)\right]$. 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

relative to the agent's consumption/wealth, then risk-diversification benefits remain for this lottery with infinitesimal winning probability.

Second, there are many 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.[28] 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 power no matter who successfully mines the block, then a successful miner who puts in very little hash power (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 benefit for normal investors in the financial market.

6.3 General Implications for Consensus Protocols

Proof-of-work protocols. Our model can help us gain better understanding of the centralizing and decentralizing forces in blockchain-based systems beyond Bitcoin, especially for

who can acquire infinitesimal hash rates is solving $\max_\epsilon \epsilon\mathbb{E}\left[u\left(\widetilde{C}+R-\epsilon p\right)\right]+(1-\epsilon)\mathbb{E}\left[u\left(\widetilde{C}-\epsilon p\right)\right]$, as he is receiving R with probability ϵ. The curvature of u enters in the valuation $p=\frac{\mathbb{E}[u(\widetilde{C}+R)-u(\widetilde{C})]}{\mathbb{E}\left[u'(\widetilde{C})\right]}$.

[28] 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.

those that rely on proof-of-work. For example, Ethereum, a major blockchain-based platform with its native cryptocurrency having a market valuation second only to Bitcoin, also relies on a proof-of-work process. For each block of transactions, be it payments or smart contracting, miners use computation powers to solve for crypto-puzzles. More specifically, the miners run the block's unique header metadata through a hash function, only changing the 'nonce value', which impacts the resulting hash value. If the miner finds a hash that matches the current target, the miner is awarded ether and broadcast the block across the network for each node to validate and add to their own copy of the ledger. Again, the proof-of-work protocol (the specific proof-of-work algorithm that Ethereum uses is called 'ethash') here makes it difficult for miners to cheat at this game, because the puzzles are hard to solve and the solutions are easy to verify. Similar to Bitcoin, the mining difficulty is readjusted automatically such that approximately every 12-15 seconds, a miner finds a block. Ethereum, along with other cryptocurrencies such as Bitcoin Cash (BCH), Litecoin (LTC), and ZCash (ZEC) that rely on PoW all witness pool formations.

(Delegated) proof-of-stake protocols A popular alternative to PoW protocols is the Proof-of-Stake (PoS) protocol, especially in light of the energy consumption concerns. The edX course titled "Blockchain for Business–An Introduction to Hyperledger Technologies" explains PoS:

"The Proof of Stake algorithm is a generalization of the Proof of Work algorithm. In PoS, the nodes are known as the validators and, rather than mining the blockchain, they validate the transactions to earn a transaction fee. There is no mining to be done, as all coins exist from day one. Simply put, nodes are randomly selected to validate blocks, and the probability of this random selection depends on the amount of stake held."

PoS systems are more environmentally friendly and efficient because the aggregate electricity consumption is much lower. Moreover, Saleh (2017) shows that once we endogenize crypto-token price and the speed to consensus, the "nothing at stake" problem that critics often cite goes away. But for a proof-of-stake method to work effectively, there still needs to be a way to select which user gets to record the next valid block. Selecting deterministically based on size alone would result in a permanent advantage for the largest stake holder. That is why "Randomized Block Selection" and the "Coin Age Based Selection" are often used in practice.

In the former, a formula which looks for the user with the combination of the lowest hash

value and the size of their stake, is used to select the validator. **Nxt** and **BlackCoin** are two examples using randomized block selection method. The coin age based system, on the other hand, selects the validator based on the coin age which is calculated by multiplying the number of days the cryptocurrency coins have been held as stake by the number of coins that are being staked. Users who have staked older and larger sets of coins have a greater chance of being assigned the block recorder. After adding a block, their coin age is reset to zero and then they must wait a minimum period of time before they can sign another block. Peercoin is a notable example that uses the coin age selection process combined with the randomized selection method.

No matter which method is used, most PoS protocols involve a reward in the form of a transaction fee and sometimes newly minted coins. Because the reward comes stochastically, 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 the stakes she has is exactly the same as in (9), with λ_m indicating the stakes allocated to pool m. All our results go through in such a case, with the caveat that consensus generation is no longer socially wasterful.

Even though many PoS protocols such as those in **QTUM**, **Reddcoin**, and **Blackcoin** can be captured by our model, we caution the readers that in practice each cryptocurrency issuer most likely customizes this system with a unique set of rules and provisions as they issue their currency or switch over from the proof-of-work system. For example, **Ethereum** currently is considering switching from PoS to Casper system which is based on Byzantine Fault Tolerance protocols (a variant of PoS); **DASH** uses a hybrid PoW and PoS protocol.

Moreover, this is a rapidly evolving industry, and there are multiple other systems and methodologies of transaction verification and consensus generation being tested and experimented with. For example, Delegated-Proof-of-Stake (DPoS) has been widely adopted to addresses the famous Nothing-at-Stake problem in PoS networks in which a small group of validators can take control of the network. **Bitshares (BTS)**, **LISK**, and **ARK** are notable examples. Stakeholders in DPos vote for delegates (typically referred to as block producers or witnesses) who maintain consensus records and share the coinbase rewards with the stakeholders in proportion to their stakes after taking their own cuts, just like the pool owners in

our model who charge a fee and give proportional rewards to individual miners.[29]

Even though our model focuses on PoW protocols, it applies to the industrial organization of players in the Blockchain consensus generation markets with risky rewards. Staking markets with PoS and DPoS are just notable examples.

6.4 Centralization in Decentralized Systems

The key innovation of the blockchain technology does not merely entail distributed ledgers or hash-linked data storage system. In fact, many technologies and applications preceding blockchain provide these functionalities already. It is the functionality of providing decentralized consensus that lies at the heart of the technology (e.g., Cong and He (2018)), and proof-of-work as manifested in Bitcoin mining plays an important role in the consensus generation process (e.g., Eyal (2015)). Given that the blockchain benefits are predicated on adequate decentralization, it is natural to worry about over-concentration in Bitcoin mining (e.g. Gervais, Karame, Capkun, and Capkun (2014)).

In this paper we have focused on the risk-sharing channel, which serves a centralizaing force, and the endogenous growth channel as a decentralizing force. There are many other channels that matter too. 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 naturally makes nodes in blockchain networks more concentrated.

Conventional wisdom in the Bitcoin community has 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. 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.[30] While sabotage concerns could affect pool sizes, it is

[29] 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/

[30] 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

outside the scope of this paper and left for future research; (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. There is no significant results when we associate 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.

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 foremost reveals that financial innovations or vehicles that improve risk-sharing can aggravate the arms race of mining, multiplying the energy consumption and social cost such as global warming and pollution. Second, we explain why blockchain systems may be adequately decentralized over time. We empirically document the market structure of Bitcoin mining pools that supports our theory. Albeit not necessarily the only explanation, ours closely ties to the risk-sharing benefit — the main driver for the emergence of mining pools in the first place. Our framework 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 highlighting in the context of cryptocurrency mining markets the roles of risk and fee on firm-size distribution.

As a first economic study on the complex industry of 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 do not consider the effect of concentration in other stages along the vertical value chain of bitcoin 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. As

processors may also attack. For a summary, see http://www.bitecoin.com/online/2015/01/11102.html.

we focus on pool formation and competition, we leave undiscussed 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

Abadi, Joseph, and Markus Brunnermeier, 2018, Blockchain economics, Discussion paper, mimeo Princeton University.

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

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.*

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.

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, .

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 Karame, Srdjan Capkun, and Vedran Capkun, 2014, Is bitcoin a decentralized currency?, *IEEE security & privacy* 12, 54–60.

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*.

Hayek, Friedrich August, 1945, The use of knowledge in society, *The American economic review* 35, 519–530.

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

Hirshlelfer, Jack, 1971, The private and social value of information and the reward to inventive activity, *The American Economic Review* 61, 561–574.

Holmström, Bengt, 1982, Moral hazard in teams, *The Bell Journal of Economics* pp. 324–340.

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

Khapko, Mariana, and Marius Zoican, 2017, 'smart' settlement, *Working Paper*.

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.

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, .

——— , 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*.

Mian, Atif, and Amir Sufi, 2015, *House of debt: How they (and you) caused the Great Recession, and how we can prevent it from happening again* (University of Chicago Press).

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.

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.

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

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*.

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.

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.

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. We prove the more general case with potential entrant pools. We start with individual miner's problem in Eq. (9). With $\Lambda_{pm} = 0$, the derivative with respect to λ_m is

$$\frac{1}{\Lambda} R(1 - f_m) e^{-\rho R(1-f_m)\frac{\lambda_m}{\Lambda_{am}}} - C \tag{20}$$

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

$$\frac{1}{\Lambda} R(1 - f_m) e^{-\rho R(1-f_m)/N} - C \tag{21}$$

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 power, 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 power 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 power or not, the global hash rate Λ has to equalize the marginal benefit of hash power with its marginal cost C, which leads to $\Lambda = \frac{R}{C} e^{-\rho R/N}$. Therefore the payoff to each miner is

$$\frac{1}{\rho\Lambda} \left[\sum_{m=1}^{M} \Lambda_{am} \left(1 - e^{-\rho R \frac{\lambda_m}{\Lambda_{am}}} \right) \right] - \frac{R}{N} e^{-\rho R/N} = \frac{1}{\rho}(1 - e^{-\rho R/N}) - \frac{R}{N} e^{-\rho R/N}, \tag{22}$$

where we have used the fact that $\sum_{m=1}^{M} \Lambda_{am} = \Lambda$, the sum of all computational power 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 $R > 0$. The exact distribution of pool size does not matter as long as $\sum_{m=1}^{M} \lambda_m = \lambda_a = \Lambda/N = \frac{R}{NC} e^{-\rho R/N}$. We note that this is not the first-best outcome because a social planner would set the hash rate to be arbitrary small to avoid any energy consumption. □

A2. Proof of Proposition 2

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

$$R(1 - f_m) = C\Lambda e^{\rho R(1-f_m)\frac{\lambda_m}{\Lambda_{am}+\Lambda_{pm}}} \leq C\Lambda e^{\rho R(1-f_m)/N} < C\Lambda e, \tag{23}$$

where the last inequality follows from Assumption 1. This implies that the RHS of (15), 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.

□

A3. Proof of Proposition 3

With $\Lambda_{pm} = \Lambda_p$ for all m, from Eq.(15) we have

$$\frac{\Lambda}{m} = \Lambda_p \frac{\rho R\left(1-f\right)}{\rho R\left(1-f\right) - N \ln \frac{R(1-f)}{C\Lambda}} \tag{24}$$

It is easy to verify that Λ is a continuous function of f, and hence each pool manager's objective function is continuous in f, and thus the optimal f^* exists within $[0,1]$. Apply Brouwer fixed-point theorem to $\in [0,1]^M$ and the mapping from $\{f_m\}_{m=1}^M$ to $\{f_m^*\}_{m=1}^M$, where $\forall m \in \{1, \cdots, M\}$, f_m^* is the optimal f_m given $\{f_k\}_{k=1,k\neq m}^M$, we have the existence of the equilibrium.

For each pool manager, her first-order condition is $0 = \pi_f + \pi_\Lambda \Lambda_f$ where

$$\pi\left(f, \Lambda(f)\right) = \frac{\Lambda_p}{\Lambda(f)} \frac{\left(1-e^{-\rho R f}\right) \rho R\left(1-f\right)}{\rho R\left(1-f\right) - N \ln \frac{R(1-f)}{C\Lambda(f)}}$$

It is easy to derive

$$\begin{aligned}
\pi_f\left(f, \Lambda(f)\right) &= \frac{\Lambda_p}{\Lambda(f)} \left[\rho R e^{-\rho R f} \frac{\rho R\left(1-f\right)}{\rho R\left(1-f\right) - N \ln \frac{R(1-f)}{C\Lambda(f)}} + \left(1-e^{-\rho R f}\right) \frac{-N \rho R \left[1 - \ln \frac{R(1-f)}{C\Lambda(f)}\right]}{\left[\rho R\left(1-f\right) - N \ln \frac{R(1-f)}{C\Lambda(f)}\right]^2} \right] \\
\pi_\Lambda\left(f, \Lambda\left(f\right)\right) &= -\frac{\Lambda_p \left(1-e^{-\rho R f}\right)}{\Lambda^2} \left[\frac{\rho R\left(1-f\right) \left[N + \rho R\left(1-f\right) - N \ln \frac{R(1-f)}{C\Lambda}\right]}{\left[\rho R\left(1-f\right) - N \ln \frac{R(1-f)}{C\Lambda}\right]^2} \right] < 0
\end{aligned}$$

Now we need to calculate and Λ_f, i.e., the impact on global hash rates by unilaterally changing the fee of one pool. From market clearing condition which holds for any fee structure $\{f_i\}$

$$\Lambda_p \sum_i \frac{\rho R\left(1-f_i\right)}{\rho R\left(1-f_i\right) - N \ln \frac{R(1-f_i)}{C\Lambda}} = \Lambda$$

we can derive (using symmetry)

$$\Lambda_f = -\frac{N \rho R \left[1 - \ln \frac{R(1-f)}{C\Lambda(f)}\right]}{\left[\rho R\left(1-f\right) - N \ln \frac{R(1-f)}{C\Lambda(f)}\right]^2} \frac{\Lambda_p}{1 - m\Lambda_p \frac{-\frac{N}{\Lambda(f)} \rho R(1-f)}{\left[\rho R(1-f) - N \ln \frac{R(1-f)}{C\Lambda(f)}\right]^2}} = -\frac{\Lambda_p N \rho R \left[1 - \ln \frac{R(1-f)}{C\Lambda(f)}\right]}{x^2 + m\Lambda_p \frac{N}{\Lambda(f)} \rho R\left(1-f\right)}$$

Define

$$x\left(f\right) \equiv \rho R\left(1-f\right) - N \ln \frac{R\left(1-f\right)}{C\Lambda}$$

then we have

$$\Lambda_f = -\frac{\Lambda_p N \rho R \left[1 - \ln \frac{R(1-f)}{C\Lambda(f)}\right]}{x^2 + m\Lambda_p \frac{N}{\Lambda(f)} \rho R\left(1-f\right)}.$$

Combining these pieces, we have any pool's FOC as $0 = \pi_f + \pi_\Lambda \Lambda_f$ which is

$$\begin{aligned} 0 &= \frac{\Lambda_p}{\Lambda}\left[\rho R e^{-\rho R f}\frac{\rho R\left(1-f\right)}{x} + \left(1-e^{-\rho R f}\right)\frac{-N\rho R\left[1-\ln\frac{R(1-f)}{C\Lambda(f)}\right]}{x^2}\right] \\ &\quad + \frac{\Lambda_p\left(1-e^{-\rho R f}\right)}{\Lambda^2}\left[\frac{\rho R\left(1-f\right)\left(N+x\right)}{x^2}\right]\frac{\Lambda_p N\rho R\left[1-\ln\frac{R(1-f)}{C\Lambda(f)}\right]}{x^2 + m\Lambda_p\frac{N}{\Lambda(f)}\rho R\left(1-f\right)} \end{aligned}$$

Cancelling terms we have

$$\begin{aligned} 0 &= e^{-\rho R f}\rho R\left(1-f\right) + \left(1-e^{-\rho R f}\right)\frac{-N\left[1-\ln\frac{R(1-f)}{C\Lambda(f)}\right]}{x} \\ &\quad + \frac{1-e^{-\rho R f}}{\Lambda}\left[\frac{\left(1-f\right)\left[N+x\right]}{x}\right]\frac{N\rho R\left[1-\ln\frac{R(1-f)}{C\Lambda(f)}\right]\Lambda_p}{x^2 + m\Lambda_p\frac{N}{\Lambda(f)}\rho R\left(1-f\right)} \end{aligned} \tag{25}$$

Plugging in (24) which says in equilibrium

$$\frac{\Lambda}{m} = \Lambda_p\frac{\rho R\left(1-f\right)}{x} \Rightarrow m\Lambda_p\frac{N}{\Lambda\left(f\right)}\rho R\left(1-f\right) = Nx, \Lambda_p\rho R\left(1-f\right) = \frac{\Lambda x}{m}$$

then (25) becomes

$$\begin{aligned} 0 &= e^{-\rho R f}\rho R\left(1-f\right) + \left(1-e^{-\rho R f}\right)\frac{-N\left[1-\ln\frac{R(1-f)}{C\Lambda(f)}\right]}{x} + \left(1-e^{-\rho R f}\right)\frac{\left[N+x\right]}{m}\frac{N\left[1-\ln\frac{R(1-f)}{C\Lambda(f)}\right]}{x^2+Nx} \\ &= e^{-\rho R f}\rho R\left(1-f\right) + \left(1-e^{-\rho R f}\right)\frac{-N\left[1-\ln\frac{R(1-f)}{C\Lambda(f)}\right]}{x} + \left(1-e^{-\rho R f}\right)\frac{1}{m}\frac{N\left[1-\ln\frac{R(1-f)}{C\Lambda(f)}\right]}{x} \\ &= e^{-\rho R f}\rho R\left(1-f\right) - \left(1-e^{-\rho R f}\right)\frac{N\left[1-\ln\frac{R(1-f)}{C\Lambda(f)}\right]}{x}\frac{m-1}{m} \end{aligned}$$

Collecting the second and the third terms, move the first term to the left hand side, we reach

$$e^{-\rho R f}\rho R\left(1-f\right) = \left(1-e^{-\rho R f}\right)\frac{N - \rho R\left(1-f\right)\left(1-\frac{m\Lambda_p}{\Lambda}\right)}{\frac{m\Lambda_p}{\Lambda}\rho R\left(1-f\right)}\frac{m-1}{m}. \tag{26}$$

In sum, the equilibrium fee and global hash rates are determined by the system of equation (24) and (26). To further simplify, let $z\left(f\right) \equiv \frac{m\Lambda_p}{\Lambda}$; then using (26) we can solve for

$$z\left(f\right) = \frac{\left(1-e^{-\rho R f}\right)\frac{m-1}{m}\left[N - \rho R\left(1-f\right)\right]}{e^{-\rho R f}\rho^2 R^2\left(1-f\right) - \left(1-e^{-\rho R f}\right)\frac{m-1}{m}}$$

As a result, based on (24) we obtain the key equation in the proposition which determines the equilibrium f:

$$\rho R\left(1-f\right)\left(1-z\left(f\right)\right) = N\ln\frac{R\left(1-f\right)z\left(f\right)}{C} - N\ln\left(m\Lambda_p\right)$$

A4. Proof of Proposition 4

Proof. (The proof is incomplete) Equations (15) and (16) imply that the owner of a pool with a positive measure of active miners maximizes

$$\pi_m = \frac{\Lambda_{pm}}{\Lambda(f_m)}\left(1-e^{-\rho R f_m}\right)\frac{\rho R(1-f_m)}{\rho R(1-f_m)+N\ln\frac{C\Lambda(f_m)}{R(1-f_m)}} \tag{27}$$

There are two scenarios. First, as shown in Lemma 1, it is possible that in equilibrium there is one entrant pool with positive measure of active hash power. In this case, locally adjusting fees by incumbents does not change the Λ. Therefore, the optimization for all incumbent pools with non-zero hash rate becomes optimizing,

$$\left(1-e^{-\rho R f_m}\right)\frac{\rho R(1-f_m)}{\rho R(1-f_m)+N\ln\frac{C\Lambda}{R(1-f_m)}}, \tag{28}$$

which is independent of Λ_{pm}. In other words, all incumbent pools charge the same fee. The proposition obviously holds.

The second scenario is that the incumbents' adjusting fees off-equilibrium moves Λ. Using FOC w.r.t. f_m and taking into consideration that the Λ in the denominator of the RHS of (15) also depends on f_m (pool owners understand adjustment to pool fees alters the global hash power), we get

Let

$$y(f_m,\Lambda(f_m)) \equiv \frac{\rho R(1-f_m)}{\rho R(1-f_m)+N\ln\frac{C\Lambda(f_m)}{R(1-f_m)}} \tag{29}$$

then

$$\frac{\partial y}{\partial \Lambda} = -\frac{N}{\Lambda}\cdot\frac{\rho R(1-f_m)}{\left[\rho R(1-f_m)+N\ln\frac{C\Lambda(f_m)}{R(1-f_m)}\right]^2} \tag{30}$$

and

$$\frac{\partial y}{\partial f_m} = -\frac{\rho R N\left(1+\ln\frac{C\Lambda(f_m)}{R(1-f_m)}\right)}{\left[\rho R(1-f_m)+N\ln\frac{C\Lambda(f_m)}{R(1-f_m)}\right]^2} \tag{31}$$

Now the FOC of (27) w.r.t. f_m gives

$$0 = \frac{d\pi_m}{df_m} = \frac{\partial \pi_m}{\partial f_m}+\frac{\partial \pi_m}{\partial \Lambda}\frac{d\Lambda(f_m)}{df_m} \tag{32}$$

$$= \frac{\Lambda_{pm}}{\Lambda}\left[\rho R e^{-\rho R f_m} y+\left(1-e^{-\rho R f_m}\right)\frac{\partial y}{\partial f_m}\right]+\Lambda_{pm}\left(1-e^{-\rho R f_m}\right)\left[\frac{1}{\Lambda}\frac{\partial y}{\partial \Lambda}\frac{d\Lambda(f_m)}{df_m}-\frac{y}{\Lambda^2}\frac{d\Lambda(f_m)}{df_m}\right] \tag{33}$$

$$= \frac{\Lambda_{pm}\rho R}{\Lambda}\cdot\frac{e^{-\rho R f_m}\rho R(1-f_m)\left[\rho R(1-f_m)+N\ln\frac{C\Lambda}{R(1-f_m)}\right]-\left(1-e^{-\rho R f_m}\right)\left[N+N\ln\frac{C\Lambda}{R(1-f_m)}\right]}{\left[\rho R(1-f_m)+N\ln\frac{C\Lambda}{R(1-f_m)}\right]^2}$$

$$-\frac{\Lambda_{pm}}{\Lambda^2}\left(1-e^{-\rho R f_m}\right)\rho R(1-f_m)\frac{N+\rho R(1-f_m)+N\ln\frac{C\Lambda(f_m)}{R(1-f_m)}}{\left[\rho R(1-f_m)+N\ln\frac{C\Lambda(f_m)}{R(1-f_m)}\right]^2}\cdot\frac{d\Lambda(f_m)}{df_m}. \tag{34}$$

From here, we get

$$-\frac{1}{\Lambda}\cdot\frac{d\Lambda(f_m)}{df_m} = \frac{N\left(1+\ln\frac{C\Lambda}{R(1-f_m)}\right)-\frac{e^{-\rho R f_m}}{1-e^{-\rho R f_m}}\rho R(1-f_m)\left[\rho R(1-f_m)+N\ln\frac{C\Lambda}{R(1-f_m)}\right]}{(1-f_m)\left[N+\rho R(1-f_m)+N\ln\frac{C\Lambda}{R(1-f_m)}\right]}. \tag{35}$$

We know that $\Lambda = \sum_{n=1}^{M} \Lambda_{pn} \cdot y(f_n, \Lambda(f_n)) \equiv \sum_{n=1}^{M} \Lambda_{pn} \cdot y_n$. Therefore,

$$\frac{d\Lambda}{df_m} = \sum_{n=1}^{M} \Lambda_{pn} \left[\frac{\partial y_n}{\partial \Lambda} \frac{d\Lambda}{df_m} + \frac{\partial y_n}{\partial f_m} \right] = \left[\sum_{n=1}^{M} \Lambda_{pn} \frac{\partial y_n}{\partial \Lambda} \right] \frac{d\Lambda}{df_m} + \Lambda_{pm} \frac{\partial y_m}{\partial f_m} \tag{36}$$

The recursive formula gives

$$\frac{d\Lambda}{df_m} = \frac{\Lambda_{pm}}{1 - \sum_{n=1}^{M} \Lambda_{pn} \frac{\partial y_n}{\partial \Lambda}} \cdot \frac{\partial y_m}{\partial f_m} \tag{37}$$

Substituting (37) into (35) and rearrange, we get

$$\begin{aligned} & \frac{\rho R}{\Lambda \left[1 - \sum_{n=1}^{M} \Lambda_{pn} \frac{\partial y_n}{\partial \Lambda} \right]} \Lambda_{pm} \\ = \quad & \frac{\left[\rho R(1-f_m) + N \ln \frac{C\Lambda}{R(1-f_m)} \right]^2}{(1-f_m) \left[N + \rho R(1-f_m) + N \ln \frac{C\Lambda}{R(1-f_m)} \right]} \cdot \left[1 - \rho R \frac{e^{-\rho R f_m}(1-f_m)}{1 - e^{-\rho R f_m}} \cdot \frac{\ln \frac{C\Lambda}{R(1-f_m)} + \frac{\rho R(1-f_m)}{N}}{\ln \frac{C\Lambda}{R(1-f_m)} + 1} \right] \end{aligned} \tag{38}$$

Now $\frac{\rho R N}{\Lambda \left[1 - \sum_{n=1}^{M} \Lambda_{pn} \frac{\partial y_n}{\partial \Lambda} \right]}$ is a constant in the cross-section of pools, therefore the LHS is linear and increasing in Λ_{pm}.

Take two pools $m = 1$ and $m = 2$ charging interior values of fees, i.e., $f_m \in (0, 1)$. Suppose $\Lambda_{p1} > \Lambda_{p2}$ and $f_1 \leq f_2$. Then LHS of (38) is bigger for Pool 1. But the RHS of (38) is independent of Λ_{pm} and is increasing in f_m and is therefore weakly larger for Pool 2, we then have a contradiction. Therefore, if $\Lambda_{p1} > \Lambda_{p2}$, it has to be $f_1 > f_2$ if the pools are charging interior fees. When they charge $f_1 = f_2 = 0$ or $f_1 = f_2 = 1$, it still holds that a larger pool does not grow disproportionally larger. The proposition follows. □

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 equivalences 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 charges a lightly lower fee and 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 1 (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 power 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 Λ 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

$$\Lambda = \frac{1}{C} R(1-f_E) e^{-\rho R(1-f_E)/N}, \tag{39}$$

and

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

where the last equality follows from (15).

In fact, pool owners choose fees to maximize

$$\Lambda_{pm} \cdot \frac{1-e^{-\rho R f_m}}{\rho\Lambda}\left[1 + \max\left\{0, \frac{N\ln[R(1-f_m)] - N\ln[C\Lambda]}{\rho R(1-f_m) + N\ln[C\Lambda] - N\ln[R(1-f_m)]}\right\}\right]. \tag{41}$$

We note that this optimization completely separates Λ_{pm} and f_m. Therefore, the optimal fee charged by all pools are the same and is independent of Λ_{pm}, which we denote by $f_I(\Lambda)$. Then (40) simplifies to

$$\Lambda \geq \left(\sum_{m=1}^{M^I} \Lambda_{pm}\right) \max\left\{1, \frac{\rho R(1-f_I)}{\rho R(1-f_I) + N\ln[C\Lambda] - N\ln[R(1-f_I)]}\right\}, \tag{42}$$

The entrant derives a utility of

$$u_E(f_E) \equiv \frac{\Lambda_{aE}(f_E)}{\rho\Lambda(f_E)}\left(1-e^{-\rho R f_E}\right) = \frac{\Lambda(f_E) - \sum_{m=1}^{M^I}(\Lambda_{am}+\Lambda_{pm})}{\rho\Lambda(f_E)}\left(1-e^{-\rho R f_E}\right) \tag{43}$$

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

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 (42) has a maximum that is bounded above by $\frac{1}{\rho}\left(1-e^{-\rho R}\right)$. We denote the maximum by

$$u(\hat{K}) \equiv \max_{f_E} u_E(f_E). \tag{44}$$

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 (43) in f_E and the fact that (43) 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

$$\frac{\left(1-e^{-\rho R f_E}\right)}{\rho\Lambda(f_E)}\left[\Lambda(f_E) - \left(\sum_{m=1}^{M^I}\Lambda_{pm}\right)\max\left\{1, \frac{\rho R(1-f_I)}{\rho R(1-f_I) + N\ln[C\Lambda] - N\ln[R(1-f_I)]}\right\}\right] = u(K) \tag{45}$$

This said, it could be the case that for such an f_E, the incumbents charge fees to attract active hash power exceeding the supposedly fixed Λ, which implies this would not be an equilibrium. As such, when K is sufficiently small, there could be entry but 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 1).

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 power 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. (39), so that $\Lambda = \frac{R}{C} e^{-\rho R/N}$. Given this, Eq. (17) 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 of fees).

Without new pool entry, the maximum global hash power satisfies

$$\Lambda = \left(\sum_{m=1}^{M^I} \Lambda_{pm} \right) \frac{\rho R}{\rho R + N \ln[C\Lambda] - N \ln R} \tag{46}$$

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

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

$$\frac{R}{\Lambda} e^{-\rho R \frac{\lambda_m}{N\lambda_m + \Lambda_{pm}}} > \frac{R}{\Lambda} e^{-\rho R \frac{1 - f_E}{N}} = \frac{C}{1 - f_E} > C \tag{47}$$

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

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 the efficient amount of hash power to them.

□

Appendix 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

Appendix C: Outcomes under Fixed Active Hashrates

We now analyze the case wherein miners cannot easily adjust the computation power in the short-run and there is also no new pool entry. Our key findings regarding pool size distribution remain robust.

Suppose each miner is endowed with a total hash power λ_a, then the active miner's problem becomes an optimal allocation of hash power into the M pools:

$$\max_{\lambda_m \geq 0} \frac{1}{\Lambda} \left[\sum_{m=1}^{M} (\Lambda_{am} + \Lambda_{pm}) \left(1 - e^{-\frac{\rho R(1-f_m)\lambda_m}{\Lambda_{am}+\Lambda_{pm}}} \right) \right], \tag{48}$$

subject to the budget constraint

$$\sum_{m=1}^{M} \lambda_m = \lambda_a. \tag{49}$$

Now $\Lambda = \sum_{m=1}^{M} (\Lambda_{am} + \Lambda_{pm}) = N\lambda_a + \sum_{m=1}^{M} \Lambda_{pm}$ is a constant. We further adapt Assumption 2 to $\rho C \left(\sum_m \Lambda_{pm} + N\lambda_a \right) > 1 - e^{-\rho R}$ which rules out solo-mining.

Given $\{\Lambda_m\}_{m=1}^{M}$ and the fee charged by other pools f_{-m}, the m-pool manager chooses f_m to maximize

$$\max_{f_m} [\Lambda_{am}(f_m, f_{-m}) + \Lambda_{pm}] \left(1 - e^{-\rho R \hat{f}_m} \right), \tag{50}$$

where $\hat{f}_m = \hat{f}(\lambda_m, \Lambda_{pm}, f_m) = \left[\frac{\Lambda_{am}}{\Lambda_{am}+\Lambda_{pm}} f_m + \frac{\Lambda_{pm}}{\Lambda_{am}+\Lambda_{pm}} \alpha(f_m) \right]$. Again, we set $\alpha(f) = f$ for easier exposition; the proofs all go through with general $\alpha(f)$.

Proposition 2 extends to the current setting.

Proposition 6. *In any equilibrium with M pools, for any two pools m and m',*

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

Proof. An active miner optimizes

$$\sum_{m=1}^{M} (\Lambda_{am} + \Lambda_{pm}) \left(1 - e^{-\rho R(1-f_m) \frac{\lambda_m}{\Lambda_{am}+\Lambda_{pm}}} \right) \tag{51}$$

In equilibrium, the marginal benefit of allocating hash rate to pool m is

$$\frac{1}{\Lambda} R(1-f_m) e^{-\rho R(1-f_m) \frac{\lambda_m}{N\lambda_m + \Lambda_{pm}}} \tag{52}$$

where we have used $\Lambda_{am} = N\lambda_m$ in equilibrium. Expression (52) is decreasing in f_m if $\rho R(1-f_m) \frac{\lambda_m}{N\lambda_m+\Lambda_{pm}} < 1$. One sufficient condition is simply $\rho R < N$, which holds by Assumption 1.

Therefore, if $\frac{\lambda_m}{\Lambda_{pm}} > \frac{\lambda_{m'}}{\Lambda_{pm'}} \geq 0$ and $f_m > f_{m'}$, (52) must be higher for pool m', which implies the miner is better off allocating some marginal hash power from pool m to pool m' (which is feasible because $\lambda_m > 0$), contradicting the fact this is an equilibrium. If in addition $\lambda_{m'} > 0$, then $\frac{\lambda_m}{\Lambda_{pm}} \geq \frac{\lambda_{m'}}{\Lambda_{pm'}} \geq 0$ would also lead to a contradiction, yielding $\frac{\lambda_m}{\Lambda_{pm}} < \frac{\lambda_{m'}}{\Lambda_{pm'}}$. □

In addition, the first statement in the proposition concerns a *Distribution Invariance in Equal-Fee Group*, which implies that without heterogeneous fees, we should not expect pool distribution to grow more dispersed or concentrated. Keep in mind that this property holds as well in our baseline case with adjustable computation power.

To see this, note that from the first part of Proposition 6, we know $-\rho R\frac{\lambda_m}{N\lambda_m+\Lambda_{pm}}$ is equal among pools charging the same fee. Replacing $-\rho R/N$ with it in the the proof of Proposition 1, then the same argument leads to that only the fee and the initial aggregate size of this group of pools matter for the active miners' allocation of hash power to this group.

Corollary 2. *Suppose that in equilibrium there is a group G of pools charging the same fee f. Then these pools grow at the same rate which is determined by f. The aggregate active hash power attracted to the group, $\sum_{m\in G}\Lambda_{am}$ depends on $\{\Lambda_{pm}, m\in G\}$ only through the pools' aggregate passive hashrate $\sum_{m\in G}\Lambda_{pm}$.*

Proof. Among the group of pools charging the same fee f, suppose the total allocation is $\hat{\lambda}_a$, then because (52) is strictly decreasing in $\frac{\lambda_m}{\Lambda_{pm}}$, we have $\frac{\lambda_m}{\Lambda_{pm}}$ being identical $\forall m$ in this group. Therefore,

$$\lambda_m = \frac{\hat{\lambda}_a}{\sum_{m'\in Group}\Lambda_{pm'}}\Lambda_{pm}. \tag{53}$$

for low enough f, and zero otherwise.

Then suppose for two particular distribution of $\{\Lambda_{pm}\}$, $\hat{\lambda}_a' > \hat{\lambda}_a''$, then $\Lambda(\hat{\lambda}_a') > \Lambda(\hat{\lambda}_a'')$, which implies that

$$\frac{1}{\Lambda}R(1-f)e^{-\rho R(1-f)\frac{\lambda_m}{N\lambda_m+\Lambda_{pm}}} = C \tag{54}$$

cannot hold for both $\hat{\lambda}_a'$ and $\hat{\lambda}_a''$. This contradiction leads to the conclusion that the aggregate active hash power attracted must equal for any two distributions and only depends on the fee f charged. □

In other words, the exact distribution of pool size for a group of pools with the same aggregate passive size, if they are charging the same fees in equilibrium, is irrelevant for the aggregate active hash power attracted to that group.

Pool sizes and fees. In equilibrium the first-order condition from the miner's optimization defines a shadow price η, so that if $\lambda_m > 0$ then

$$\eta = \rho R(1-f_m)e^{-\rho R(1-f_m)\frac{\lambda_m}{N\lambda_m+\Lambda_{pm}}}, \tag{55}$$

We focus on the case where $\lambda_m > 0$, $\forall m$.[31] At the same time $\sum_{m=1}^{M}\lambda_m = \lambda_a$. Denote the solution as $\eta^*(f_m, \Lambda_{pm}, m = 1, 2, \cdots, M)$. Then the pool owner m's optimization can be transformed into

$$\max_{f_m}\frac{\rho R(1-f_m)}{\rho R(1-f_m) + N\ln\eta^* - N\ln[\rho R(1-f_m)]}\left(1-e^{-\rho R f_m}\right), \tag{56}$$

Before discussing the general case, let us first examine the case of $M = 2$ for analytical solutions and basic intuition.

A two-pool example. Suppose there are only two pools.

Proposition 7. *In an equilibrium whereby active miners only allocate hash rates between two pools (Pools 1 and 2), $\Lambda_{p1} \geq (>)\Lambda_{p2}$ implies $f_1 \geq (>) f_2$ in equilibrium.*

Proof. We only discuss the $\geq$ case because the $>$ case is almost identical. We use proof by contradiction. Suppose that $\Lambda_{p1} \geq \Lambda_{p2}$ but $f_1 < f_2$.

[31] If the constraint $\lambda_m = 0$ is binding then there is another Lagrange multiplier for this constraint.

Recall that $\hat{f}_m = \hat{f}(\lambda_m, \Lambda_{pm}, f_m) = \left[\frac{N\lambda_m}{N\lambda_m+\Lambda_{pm}} f_m + \frac{\Lambda_{pm}}{N\lambda_m+\Lambda_{pm}}\alpha(f_m)\right]$. From Proposition 6, $f_1 < f_2$ implies $\frac{N\lambda_1}{N\lambda_1+\Lambda_{p1}} \geq \frac{N\lambda_2}{N\lambda_2+\Lambda_{p2}}$. Given that $\alpha(f) \geq f$ and is weakly increasing in f, one can easily show that $\hat{f}_1 < \hat{f}_2$.

Now no deviations from equilibria gives

$$(N\lambda_1 + \Lambda_{p1})\left(1 - e^{-\rho R\hat{f}_1}\right) \geq \left(\frac{\Lambda_{p1}\Lambda_A}{\Lambda_{p1}+\Lambda_{p2}} + \Lambda_{p1}\right)\left(1 - e^{-\rho R\hat{f}_2}\right)$$

$$(N\lambda_2 + \Lambda_{p2})\left(1 - e^{-\rho R\hat{f}_2}\right) \geq \left(\frac{\Lambda_{p2}\Lambda_A}{\Lambda_{p1}+\Lambda_{p2}} + \Lambda_{p2}\right)\left(1 - e^{-\rho R\hat{f}_1}\right),$$

where Λ_{A1} and Λ_{A2} are the *total* allocation from all active miners to pool 1 and 2 when they charge equilibrium fees f_1 and f_2, respectively. Notice that $N\lambda_1 + N\lambda_2 = \Lambda_A$, we thus get

$$(\Lambda_A + \Lambda_{p1} + \Lambda_{p2}) \geq \left(\frac{\Lambda_{p1}\Lambda_A}{\Lambda_{p1}+\Lambda_{p2}} + \Lambda_{p1}\right)\frac{1 - e^{-\rho R\hat{f}_2}}{1 - e^{-\rho R\hat{f}_1}} + \left(\frac{\Lambda_{p2}\Lambda_A}{\Lambda_{p1}+\Lambda_{p2}} + \Lambda_{p2}\right)\frac{1 - e^{-\rho R\hat{f}_1}}{1 - e^{-\rho R\hat{f}_2}}$$

Factoring out $\Lambda_A + \Lambda_{p1} + \Lambda_{p2}$ and multiply $\Lambda_{p1} + \Lambda_{p2}$ on both sides we have

$$\Lambda_{p1} + \Lambda_{p2} \geq \Lambda_{p1}\frac{1 - e^{-\rho R\hat{f}_2}}{1 - e^{-\rho R\hat{f}_1}} + \Lambda_{p2}\frac{1 - e^{-\rho R\hat{f}_1}}{1 - e^{-\rho R\hat{f}_2}},$$

which cannot possibly hold because $\hat{f}_2 > \hat{f}_1$ and $\Lambda_{p1} \geq \Lambda_{p2}$.

□

Proposition 7 implies that a (weakly) larger pool charges a (weakly) higher fee. The main intuition again derives from the arms-race effect and market power. When the pool managers decide on their fees, they are facing a demand curve aggregated from individual active miners' allocation problem under their budget constraint. Intuitively, a larger pool with a bigger Λ_{pm} provides greater diversification benefit, thus faces a less elastic demand curve. This implies that an active miner still wants to allocate significant amount of hash rates to it despite the higher fee charged by the larger pool, giving rise to our claimed result.

Combined with Proposition 6, the result that $\Lambda_{p1} > \Lambda_{p2}$ leads to $\frac{\Lambda_{a1}}{\Lambda_{p1}} \leq \frac{\Lambda_{a2}}{\Lambda_{p2}}$, i.e., a larger pool has a lower growth rate. Therefore, the market power of mining pools creates a natural force that prevents larger pools from becoming more dominant.

Dominant pools and equilibrium fees. Relating to the concern of "51% attack" by a dominant pool, we also analyze a case where one larger pool dominates other pools of similar size.

Proposition 8. *If $\Lambda_{p1} > \Lambda_{p2} = \Lambda_{p3} = \cdots = \Lambda_{pM}$, then in a symmetric equilibrium $f_1 > f_m$, $\forall m = 2, 3, \cdots, M$. As a result, the largest pool 1 grows slower than the rest of pools.*

Proof. In a symmetric equilibrium pool 2 through M charge the same fee. We denote it by f_2 and prove the proposition by contradiction. Similar to Proposition 7, suppose $f_1 \leq f_2$, then for $m = 2, \cdots, M$, the following holds.

$$(N\lambda_1 + \Lambda_{p1})\left(1 - e^{-\rho R\hat{f}_1}\right) \geq \left(\frac{\Lambda_{p1}\Lambda_A}{\Lambda_{p1}+(M-1)\Lambda_{p2}} + \Lambda_{p1}\right)\left(1 - e^{-\rho R\hat{f}_2}\right) \tag{57}$$

$$(N\lambda_m + \Lambda_{pm})\left(1 - e^{-\rho R\hat{f}_2}\right) \geq \left(\frac{\Lambda_{pm}\Lambda_{1\&m}}{\Lambda_{p1}+\Lambda_{pm}} + \Lambda_{p2}\right)\left(1 - e^{-\rho R\hat{f}_1}\right) \tag{58}$$

$$\geq \left(\frac{\Lambda_{p1}\Lambda_{p2}}{\Lambda_{p1}+(M-1)\Lambda_{p2}} + \Lambda_{p2}\right)\left(1 - e^{-\rho R\hat{f}_1}\right), \tag{59}$$

where the last inequality follows from that $\Lambda_{1\&m}$ is the total miner allocation to pool 1 and pool m when they both charge f_1, and is therefore larger than $\frac{\Lambda_{p1}+\Lambda_{pm}}{\Lambda_{p1}+(M-1)\Lambda_{p2}}$ because as a group, pool 1 and pool m gets an overall allocation as if they are charging a lower fee than the rest of the pools.

Then following the same argument as in the proof of Proposition 7, we arrive at a contradiction. Therefore, $f_1 > f_2$. □

The proposition shows that even with M pools, if one pool dominates and other pools are of similar size, then the dominant pool would charge a higher fee and grow at a slower rate. In fact, the proof equally applies to the scenario whereby there are two classes of pool, one with larger size and one with smaller size. The former always charge higher fees and grow at a slower rate.

Numerical illustrations of general cases. We present the numerical solution in Figure 5 for the general case of $N = 3$, with $\Lambda_{p1} > \Lambda_{p2} > \Lambda_{p3}$. Again, due to the same economic forces that we explained in the earlier section with two pools or a large dominant pool, Figure 5 illustrates that the equilibrium pool fee increases in pool size, and larger pools grow slower.

Figure 5: **Comparative Statics of Pool Fees and Growth**

Equilibrium fees f_i's and the pool growth rate $\Lambda_{ai}/\Lambda_{pi}$'s, $i \in 1, 2, 3$, are plotted against miner risk aversion ρ. The baseline parameters are: $R = 1 \times 10^5, \lambda_a = 5 \times 10^4$, $N = 50$, $\Lambda_{p1} = 5 \times 10^5, \Lambda_{p2} = 3 \times 10^5, \Lambda_{p3} = 1 \times 10^5$ and $\rho \in \left[1 \times 10^{-5}, 3 \times 10^{-5}\right]$.