Decentralized Mining in Centralized Pools

Will Cong           Zhiguo He           Jiasun Li

UChicago            UChicago & NBER     George Mason

Harvard, January 2019
Decentralized Consensus: the Bitcoin Example

- Digital/online transactions & central record-keeper
  - Visa Inc. for credit card transactions, central banks for clearing, etc.

- Bitcoin: a **decentralized** cryptocurrency.

- Generating/maintaining decentralized consensus
  - Cong and He (2018): endogenous costs of generating such consensus via information
  - Mining and Proof-of-Work (PoW): open tournament for miners (independent computers) with rewards
    - But, mining is a zero-sum game. **Arms race**
  - Rewards only valid if endorsed by subsequent miners → honest recording → no double-spending.
  - Open access and trustless → little market power for intermediaries
Rise of Mining Pools

- Bitcoin’s (PoW or other protocols) well-functioning relies on adequate decentralization.

- Decentralization: *technological* possibility vs *economic* reality?

- Miners pool in reality
  - “Pooled mining” completely dominates “solo mining”
    - Technologically, no increasing return to scale
    - A first-order benefit: risk sharing within the pool
  - Concerns over sustainability (51% attack, selfish mining, etc.)
  - We offer fresh economic analyses to
    - clarify certain fallacies
    - highlight one important mechanism
Evolution of Bitcoin Mining

The evolution of Bitcoin mining pool size shares

- hashrates rise with pools...
- pools grow first then slow down...
Preview of Results

- Risk-aversion $\implies$ pooling: significant risk-sharing benefits
  - Diversifying via pools improves (risk-averse) individual payoff but worsens the arms race of mining, quantitatively significant
  - **Links egregious energy use with pools;** financial innovation aggravates arms race (5$\sim$10 times)

- Risk-aversion $\implies$ pools; but $\not\implies$ pools to merge/centralization
  - Miners can join multiple pools, diversify by themselves
  - M&M: investors diversify themselves $\implies$ no need for firms to merge

- An equilibrium model of the mining industry
  - Miners acquire and allocate hash power
  - Pool owners (enter and) charge fees
  - Pool’s initial passive hash rates as an IO friction, monopolistic competition (robust to entry)

- Empirical evidence from Bitcoin data
Outline

- Introduction
- Mining Pools
- Model & Equilibrium
- Empirical Analysis
- Discussion & Conclusion
Bitcoin Mining 101

- Miners repeatedly compete to record recent transactions (aka attaching a block to the chain)
- Winner receives coinbase (currently 12.5BTC) + transactions fees
- A tournament via enumeration through solving cryptographic puzzles
  - Hash(solution, block) has adequate leading zeros
  - every miner/pool solves a different problem
- Difficulty adjustment: harder problem given greater global hash rates
  - ~1 block/10 mins; my mining hurts others’ winning probability
  - The exact source of arms race (negative) externality
Characterizing (Solo) Mining Payoffs

Solution Poisson arrives with rate proportional to a miner’s share of global hash rates

- Miner’s payoff:

\[ X_{solo} = \tilde{B}_{solo} R - c(\lambda_A, T), \text{ where} \]

- \( \tilde{B}_{solo} \sim \text{Poisson} \left( \frac{1}{D} \frac{\lambda_A}{\Lambda} T \right) \): # blocks found in \( T \)
- \( \Lambda \): global hashrate
- \( D = 60 \times 10 \text{ seconds} \): constant
- \( R \): dollar reward per block (coinbase \( \times \) Bitcoin price + TX fees)
- \( c(\lambda_A, T) = c\lambda_A T \): cost of operation/electricity
Characterizing (Solo) Mining Payoffs

Solution Poisson arrives with rate proportional to a miner’s share of global hash rates

- Miner’s payoff:

\[ X_{\text{solo}} = \tilde{B}_{\text{solo}} R - c(\lambda_A, T), \]

where

- \( \tilde{B}_{\text{solo}} \sim \text{Poisson} \left( \frac{1}{D} \frac{\lambda_A}{\Lambda} T \right) \): # blocks found in \( T \)
- \( \Lambda \): global hashrate
- \( D = 60 \times 10 \) seconds: constant
- \( R \): dollar reward per block (coinbase \( \times \) Bitcoin price + TX fees)
- \( c(\lambda_A, T) = c\lambda_A T \): cost of operation/electricity
Rise of Mining Pools

A (proportional) mining pool

- combines multiple miners’ hash rates to solve one puzzle
- distributes rewards in proportion to hashrate contributions

Over $T$, payoff to a miner with $\lambda_A$ who joins a (free) pool with $\Lambda_B$ is

$$X_{\text{pool}} = \frac{\lambda_A}{\lambda_A + \Lambda_B} \tilde{B}_{\text{pool}} R - c(\lambda_A, T),$$

where

$$\tilde{B}_{\text{pool}} \sim \text{Poisson} \left( \frac{1}{D} \frac{\lambda_A + \Lambda_B}{\Lambda} T \right)$$
Rise of Mining Pools

A (proportional) mining pool
- combines multiple miners’ hash rates to solve one puzzle
- distributes rewards in proportion to hashrate contributions

Over $T$, payoff to a miner with $\lambda_A$ who joins a (free) pool with $\Lambda_B$ is

$$X_{pool} = \frac{\lambda_A}{\lambda_A + \Lambda_B} \tilde{B}_{pool} R - c(\lambda_A, T),$$

where

$$\tilde{B}_{pool} \sim \text{Poisson} \left( \frac{1}{D} \frac{\lambda_A + \Lambda_B}{\Lambda} T \right)$$
Solo vs Pool

A miner with $\lambda_A$ over period $T$:

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

$$X_{pool} = \frac{\lambda_A}{\lambda_A + \Lambda_B} \tilde{B}_{pool} R - c(\lambda_A, T), \tilde{B}_{pool} \sim \text{Poisson} \left( \frac{1}{D} \frac{\lambda_A + \Lambda_B}{\Lambda} T \right)$$

$X_{pool}$ second-order stochastically dominates $X_{solo}$, risk-diversification benefit
Illustration of Significant Risk-sharing Benefits

- $\lambda_A = 13.5 \text{(TH/s)}$: Bitmain Antminer S9 ASIC miner
- $\lambda_B = 3,000,000 \text{(TH/s)}$: scale of one large mining pool
- $R = $100,000 \((12.5 + \sim 0.5)BTC/\text{block} \times $8K/BTC \Rightarrow $104K\)
- CARA $\rho = .00002$ (CRRA of 2 / wealth of $100K$
- $T = 3600 \times 24s$: one day

We have

- $CE_{solo} = $4.00 vs $CE_{pool} = $9.26, a 131% boost!
- Quantitatively large risk-sharing benefit even for a small pool: $\Lambda_B = 13.5$, about $\sim 20\%$ of boost
- Basic finance insights: quantitatively large diversification benefit in the first 20 stocks

Caveat: miners are deciding how to allocate across pools, not whether or not join pools
A pool manager
- coordinates hash rates and charges pool fees
- just like a firm but can contract on “effort”

Contracting variable
- miner’s hashrate can be closely approximated by **partial solutions**
  - $\text{Hash}(\text{partial solution}, \text{block})$ also below a threshold
    but much more relaxed than that required for a **solution**
- hashrate (effort) is essentially **observable** by counting partial solutions
- in the context of contracting: no moral hazard issue, only risk sharing (Holmstrom, 1979)!
Mining Pool: Structure and Fee Contract

∼10 slightly different contracts in three categories:

1. proportional: $\frac{\lambda_A}{\lambda_A + \lambda_B} (1 - f) \tilde{B} R$, with $\tilde{B} \sim \text{Poisson}(\frac{1}{D} \frac{\lambda_A + \lambda_B}{\Lambda} T)$
   - output-based wage

2. pay per share (PPS): $r \cdot \lambda_A$ where $r = \frac{RT}{DA} (1 - f_{PPS})$
   - hourly-based wage

3. cloud mining: exactly the opposite of PPS

We focus on proportional pools
- ∼70% of pools adopt (28% exclusively)
- PPS/cloud only relevant for heterogeneous risk aversions
## Evolution of Pool Sizes and Fee Contracts

<table>
<thead>
<tr>
<th>Year</th>
<th>Hashrate (PH/s) (A)</th>
<th># of Pools (B)</th>
<th>Top 5 (%) (C)</th>
<th>Avg Fee (Size.W.) (%) (D)</th>
<th># Frac. Prop (%) (E)</th>
<th>Fee (%)</th>
<th>Prop. Ave.</th>
<th>Prop. Ave.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Top 5</td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td>0.01</td>
<td>8</td>
<td>7.63</td>
<td>0.57</td>
<td>87.12</td>
<td>0.28</td>
<td>0.28</td>
<td>0.28</td>
</tr>
<tr>
<td>2012</td>
<td>0.02</td>
<td>15</td>
<td>34.66</td>
<td>2.71</td>
<td>61.25</td>
<td>0.66</td>
<td>1.76</td>
<td>0.65</td>
</tr>
<tr>
<td>2013</td>
<td>1.48</td>
<td>23</td>
<td>71.01</td>
<td>2.73</td>
<td>62.57</td>
<td>1.58</td>
<td>2.29</td>
<td>1.16</td>
</tr>
<tr>
<td>2014</td>
<td>140.78</td>
<td>33</td>
<td>70.39</td>
<td>0.88</td>
<td>70.50</td>
<td>1.33</td>
<td>1.13</td>
<td>0.88</td>
</tr>
<tr>
<td>2015</td>
<td>403.61</td>
<td>43</td>
<td>69.67</td>
<td>1.51</td>
<td>77.92</td>
<td>1.10</td>
<td>1.31</td>
<td>0.84</td>
</tr>
<tr>
<td>2016</td>
<td>1,523.83</td>
<td>36</td>
<td>75.09</td>
<td>2.50</td>
<td>77.14</td>
<td>1.48</td>
<td>2.15</td>
<td>0.97</td>
</tr>
<tr>
<td>2017</td>
<td>6,374.34</td>
<td>43</td>
<td>62.25</td>
<td>1.67</td>
<td>78.89</td>
<td>2.00</td>
<td>1.43</td>
<td>1.42</td>
</tr>
</tbody>
</table>
## Current Contract Sample

<table>
<thead>
<tr>
<th>Name</th>
<th>Reward Type</th>
<th>Transaction fees</th>
<th>Prop. Fee</th>
<th>PPS Fee</th>
</tr>
</thead>
<tbody>
<tr>
<td>AntPool</td>
<td>PPLNS &amp; PPS</td>
<td>kept by pool</td>
<td>0%</td>
<td>2.50%</td>
</tr>
<tr>
<td>BTC.com</td>
<td>FPPS</td>
<td>shared</td>
<td>4%</td>
<td>0%</td>
</tr>
<tr>
<td>BCMonster.com</td>
<td>PPLNS</td>
<td>shared</td>
<td>0.50%</td>
<td>0%</td>
</tr>
<tr>
<td>Jonny Bravo’s</td>
<td>PPLNS</td>
<td>shared</td>
<td>0.50%</td>
<td>0%</td>
</tr>
<tr>
<td>Slush Pool</td>
<td>Score</td>
<td>shared</td>
<td>2%</td>
<td></td>
</tr>
<tr>
<td>BitMinter</td>
<td>PPLNSG</td>
<td>shared</td>
<td>1%</td>
<td></td>
</tr>
<tr>
<td>BTCC Pool</td>
<td>PPS</td>
<td>kept by pool</td>
<td>0%</td>
<td>2.00%</td>
</tr>
<tr>
<td>BTCDig</td>
<td>DGM</td>
<td>kept by pool</td>
<td>0%</td>
<td></td>
</tr>
<tr>
<td>btcmp.com</td>
<td>PPS</td>
<td>kept by pool</td>
<td>0%</td>
<td>4%</td>
</tr>
<tr>
<td>Eligius</td>
<td>CPPSRB</td>
<td>shared</td>
<td>0%</td>
<td></td>
</tr>
<tr>
<td>F2Pool</td>
<td>PPS</td>
<td>kept by pool</td>
<td>0%</td>
<td>3%</td>
</tr>
<tr>
<td>GHash.IO</td>
<td>PPLNS</td>
<td>shared</td>
<td>0%</td>
<td></td>
</tr>
<tr>
<td>Give Me COINS</td>
<td>PPLNS</td>
<td>shared</td>
<td>0%</td>
<td></td>
</tr>
<tr>
<td>KanoPool</td>
<td>PPLNSG</td>
<td>shared</td>
<td>0.90%</td>
<td></td>
</tr>
<tr>
<td>Merge Mining Pool</td>
<td>DGM</td>
<td>shared</td>
<td>1.50%</td>
<td></td>
</tr>
<tr>
<td>Multipool</td>
<td>Score</td>
<td>shared</td>
<td>1.50%</td>
<td></td>
</tr>
<tr>
<td>P2Pool</td>
<td>PPLNS</td>
<td>shared</td>
<td>0%</td>
<td></td>
</tr>
<tr>
<td>MergeMining</td>
<td>PPLNS</td>
<td>shared</td>
<td>1%</td>
<td></td>
</tr>
</tbody>
</table>

*Source: Bitcoin wiki*
Outline

- Introduction
- Mining Pools
- Model & Equilibrium
- Empirical Analysis
- Discussion & Conclusion
Model Setup

- Static game, CARA $u(x) = \frac{1}{\rho} (1 - e^{-\rho x})$

- $N$ measure of active miners acquire hash rate $\lambda_a$ at a cost of $C$, taking equilibrium $\{f_m\}_{m=1}^M$ as given
  - Symmetric equilibrium: all active miners same allocation

- $M$ pool managers set fees $f_m$ to compete

- “Friction”: pool $m$ endowed with passive hash rates $\Lambda_{pm} \geq 0$
  - “Loyal fans”, complementary services, proprietary hash power (mining factory)
  - Key to monopolistic competition
  - Empirical link to initial pool size
Model Setup

- Static game, CARA $u(x) = \frac{1}{\rho} (1 - e^{-\rho x})$

- $N$ measure of active miners acquire hash rate $\lambda_x$ at a cost of $C$, taking equilibrium $\{f_m\}_{m=1}^M$ as given
  - Symmetric equilibrium: all active miners same allocation

- $M$ pool managers set fees $f_m$ to compete

- “Friction”: pool $m$ endowed with passive hash rates $\Lambda_{pm} \geq 0$
  - “Loyal fans”, complementary services, proprietary hash power (mining factory)
  - Key to monopolistic competition
  - Empirical link to initial pool size
Active Miner’s Problem

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

(1)

the problem reduces to

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

(2)

where the global hash rate \( \Lambda \) is

\[
\Lambda = \sum_{m=1}^{M} (\Lambda_{am} + \Lambda_{pm}).
\]  

(3)
Active Miner’s Problem

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

(1)

the problem reduces to

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

(2)

where the global hash rate \( \Lambda \) is

\[
\Lambda = \sum_{m=1}^{M} (\Lambda_{am} + \Lambda_{pm}).
\]  

(3)
Pool Managers’ Problem

Given \( \{ \Lambda_{pm} \}_{m=1}^{M} \) and \( f_{-m} \), manager \( m \) with fee \( f_m \) has a cashflow of

\[
\tilde{B}_{pool,m} \cdot Rf_m, \text{ with } \tilde{B}_{pool,m} \sim \text{Poisson} \left( \frac{1}{D} \frac{\Lambda_{am} + \Lambda_{pm}}{\Lambda} T \right)
\]

Any pool owner’s problem becomes

\[
\max_{f_m} \frac{\Lambda_{am}(f_m) + \Lambda_{pm}}{\rho\Lambda(f_m, f_{-m})} \left( 1 - e^{-\rho Rf_m} \right)
\]  \hspace{1cm} (4)

- Each managers takes into account the effect of his own fees \( f_m \) on global hash rates \( \Lambda \)
- ......infinitesimal miners do not
Pool Managers’ Problem

Given $\{\Lambda_{pm}\}_{m=1}^{M}$ and $f_{-m}$, manager $m$ with fee $f_{m}$ has a cashflow of

$$\tilde{B}_{pool,m} \cdot Rf_{m}, \text{ with } \tilde{B}_{pool,m} \sim \text{Poisson}\left(\frac{1}{D} \frac{\Lambda_{am} + \Lambda_{pm}}{\Lambda} T\right)$$

Any pool owner’s problem becomes

$$\max_{f_{m}} \frac{\Lambda_{am}(f_{m}) + \Lambda_{pm}}{\rho \Lambda(f_{m}, f_{-m})} \left(1 - e^{-\rho Rf_{m}}\right)$$  \hspace{1cm} (4)

- Each manager takes into account the effect of his own fees $f_{m}$ on global hash rates $\Lambda$
- …..infinitesimal miners do not
Equilibrium Definition

A symmetric equilibrium is a collection of \( \{f_m\}_{m=1}^{M} \) and \( \{\lambda_m\}_{m=1}^{M} \) so that

- **Optimal fees:** \( \{f_m\}_{m=1}^{M} \) solves each manager’s problem
- **Optimal hash rates allocation:** given \( \{f_m\}_{m=1}^{M}, \{\lambda_m\}_{m=1}^{M} \) solve each active miner’s problem
- **Market clearing:** \( \Lambda_{am} = N\lambda_m \)

- initial size distribution \( \{\Lambda_{pm}\}_{m=1}^{M} \), resulting size distribution \( \{\Lambda_{am} + \Lambda_{pm}\}_{m=1}^{M} \). Pool growth \( \frac{\Lambda_{am}}{\Lambda_{pm}} \)
A Frictionless Benchmark: $\Lambda_{pm} = 0$

Proposition (Irrelevance of Pool Size Distribution)

- $f_m = 0$ for all $m$
- any allocation $\{\lambda_m\}_{m=1}^M$ with $\Lambda = N \sum_{m=1}^M \lambda_m = \frac{R}{C} e^{-\rho R/N}$

- Miners have perfect risk sharing by themselves
- M$\$M: why a larger pool when individuals can diversify freely?
  ▶ Fallacy of “risk-diversification $\implies$ pools merge/centralization”

- **Mining arms race**: in our simplified Economic modeling, mining energy is a waste
  ▶ PoW protocol has other benefits not captured by this model
- Dark side of pools: marginal benefit of $\frac{R}{C} e^{-\rho R/N}$ with full risk-sharing, v.s. $\Lambda = \frac{R}{C} e^{-\rho R}$ with solo
Equilibrium with Passive Hash Rates

Active miner’s FOC:

\[
\frac{R(1 - f_m)}{\Lambda} \left( e^{-\rho R(1-f_m)\frac{\lambda_m}{\Lambda_{am} + \Lambda_{pm}}} \right) = C
\]

(5)

- Larger pools attract more allocation for better diversification (the second term)
- Marginal benefit of very first unit \( (\lambda_m = 0) \) is risk-neutral valuation (the first term)
  - In equilibrium any pool can attract some miners always. Like monopolistic competition

In equilibrium \( N\lambda_m = \Lambda_{am} \). Hence

\[
\frac{\lambda_m}{\Lambda_{pm}} = \frac{\ln \frac{R(1-f_m)}{C\Lambda}}{\rho R(1 - f_m) - N \ln \frac{R(1-f_m)}{C\Lambda}}
\]

(6)
Equilibrium with Passive Hash Rates

Active miner’s FOC:

\[
\frac{R(1 - f_m)}{\Lambda} \cdot e^{-\rho R(1-f_m)\frac{\lambda_m}{\Lambda_{am}+\Lambda_{pm}}} = C
\]

- Larger pools attract more allocation for better diversification (the second term)
- Marginal benefit of very first unit ($\lambda_m = 0$) is risk-neutral valuation (the first term)
  - In equilibrium any pool can attract some miners always. Like monopolistic competition

In equilibrium $N\lambda_m = \Lambda_{am}$. Hence

\[
\frac{\lambda_m}{\Lambda_{pm}} = \frac{\ln \frac{R(1-f_m)}{C\Lambda}}{\rho R(1 - f_m) - N \ln \frac{R(1-f_m)}{C\Lambda}}
\]
Main Results Overview

**Proposition**

*Same fee, same growth; higher fee, lower growth.*

- if \( f_m = f_{m'} \), then \( \Lambda_{am} \Lambda_{pm} = \Lambda_{am'} \Lambda_{pm'} \);
- if \( f_m > f_{m'} \) then \( \Lambda_{am} \Lambda_{pm} < \Lambda_{am'} \Lambda_{pm'} \).

**Main Results**

1. **Social cost of pools**
   - Equilibrium of symmetric pools (\( \Lambda_{pm} = \Lambda_{p} \))
   - Oligopolistic pools take arms race into account, charge positive fees
     \( \implies \) less global hash rates than full risk-sharing but more than solo

2. **What if heterogeneous pools: Larger pools charge higher fees?**
   - Yes, because larger pools take into account of arms race effect more
Main Results Overview

**Proposition**

*Same fee, same growth; higher fee, lower growth.*

- If \( f_m = f_m' \), then \( \frac{\Lambda_{am}}{\Lambda_{pm}} = \frac{\Lambda_{am'}}{\Lambda_{pm'}} \);
- If \( f_m > f_m' \) then \( \frac{\Lambda_{am}}{\Lambda_{pm}} < \frac{\Lambda_{am'}}{\Lambda_{pm'}} \).

Main Results

1. **Social cost of pools**
   - Equilibrium of symmetric pools (\( \Lambda_{pm} = \Lambda_p \))
   - Oligopolistic pools take arms race into account, charge positive fees
     \( \iff \) less global hash rates than full risk-sharing but more than solo

2. **What if heterogeneous pools: Larger pools charge higher fees?**
   - Yes, because larger pools take into account of arms race effect more
Social Cost of Mining Pools

\[ R = 1 \times 10^5, \quad N = 10, \quad M = 2, \quad C = 0.00204, \quad \text{and} \quad \rho = 1 \times 10^{-5}. \]
Pool Evolution: Larger $\Lambda_{pm}$, Lower $\frac{\Lambda_{am}}{\Lambda_{pm}}$

\[ R = 1 \times 10^5, \; \lambda_a = 5 \times 10^4, \; N = 10, \; \Lambda_{p1} = 5 \times 10^5, \; \Lambda_{p2} = 3 \times 10^5, \; \Lambda_{p3} = 1 \times 10^5, \; C = 0.00204, \; \text{and} \; \rho = 2 \times 10^{-5}. \]
Outline

- Introduction
- Mining Pools
- Model & Equilibrium
- Empirical Analysis
- Discussion & Conclusion
Empirical Evidence: Data and Methodology

Data on pool size (i.e., hashrate share) evolution
- estimated from block relaying records (weekly)
- the newly mined blocks divided by total blocks mined globally (a widely used estimator)

Data on pool fee/reward type evolution
- Bitcoin Wiki: Comparison of mining pools
- the entire Wiki revision history

What we do
1. beginning of every quarter, sort pools into deciles based on start-of-quarter hashrate share
2. calculate avg. pool share quarterly growth rates and average fees for each decile
3. investigate relationships in three two-years spans (i.e., 2012-2013, 2014-2015, and 2016-2017)
Empirical Evidence: Results

Panel A: $\Delta \log \text{Share} \text{ vs } \log \text{Share}$

- **2012 - 2013**: t-stat = -3.34
- **2014 - 2015**: t-stat = -3.80
- **2016 - 2017**: t-stat = -2.87
Empirical Evidence: Results

Panel B: Proportional Fee vs log Share

- 2012 - 2013: t-stat = 3.62
- 2014 - 2015: t-stat = 2.08
- 2016 - 2017: t-stat = 5.50
Outline

- Introduction
- Mining Pools
- Model & Equilibrium
- Empirical Analysis
- Discussion & Conclusion
Entry and Market Power

- $M^I$ incumbents; entrants ($\Lambda_{pm} = 0$) pay $K$ to enter.

**Proposition (Market Power of Incumbent Pools)**

At most one pool enters. Incumbent pools ($\Lambda_{pm} > 0$) always charge $f_m > 0$ and attract $\Lambda_{am} > 0$, even with $K = 0$ (free entry).

- Incumbents are with certain market power; monopolistic competition
  - If no fee, miners get risk-neutral mining reward $\frac{R}{\Lambda}$ as marginal benefit starting from $\lambda_m = 0$
- Incumbent positive rents $\rightarrow$ no full risk-sharing (among active miners)
Entry and Market Power

- $M^I$ incumbents; entrants ($\Lambda_{pm} = 0$) pay $K$ to enter.

Proposition (Market Power of Incumbent Pools)

At most one pool enters. Incumbent pools ($\Lambda_{pm} > 0$) always charge $f_m > 0$ and attract $\Lambda_{am} > 0$, even with $K = 0$ (free entry).

- Incumbents are with certain market power; monopolistic competition
  - If no fee, miners get risk-neutral mining reward $\frac{R}{\Lambda}$ as marginal benefit starting from $\lambda_m = 0$
- Incumbent positive rents $\rightarrow$ no full risk-sharing (among active miners)
Risk and Other Protocols

- Risk
  - diversifying idiosyncratic risk (which is our focus) is the foundation of modern finance
  - infinitesimal mining (\(\epsilon\) chance of a huge lottery win) still has non-negligible risk discount
  - the fallacy of large numbers (diversify over time)
  - can easily introduce aggregate risk in \(R\)

- Other consensus generation protocols (than PoW)? Still apply
  - Proof-of-Stake (PoS, DPoS)
  - As long as the exact recordkeeper is randomized each round (with probability depending on stake, not work)

- Other centralizing & decentralizing forces
Conclusion

1. A theory of mining pools
   - Financial innovation that improve risk-sharing aggravates mining arms race, contributing to egregious energy consumption

2. Risk-sharing $\implies$ pools, but diversification across pools sustains decentralization
   - MM insight, IO insight $\implies$ Blockchain sustainability
   - Same force, other factors can be added
   - Empirical evidence: Bitcoin mining industry structure

3. Theory
   - IO of crypto-mining/consensus generation markets
   - FinTech/gig/sharing economy; decentralized systems
   - Monopolistic competition with risk aversion and externality