Decentralized Mining in Centralized Pools

Will Cong — Cornell
Zhiguo He — UChicago & NBER
Jiasun Li — George Mason

December 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 $\rightarrow$ honest recording $\rightarrow$ no double-spending
    - Biais, Bisiere, Bouvard, and Casamatta (2018)
  - Open access and trustless $\rightarrow$ little market power for intermediaries

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 $\rightarrow$ honest recording $\rightarrow$ no double-spending
    - Biais, Bisiere, Bouvard, and Casamatta (2018)
  - Open access and trustless $\rightarrow$ little market power for intermediaries

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
    - ⋆ Biais, Bisiere, Bouvard, and Casamatta (2018)
  - Open access and trustless → little market power for intermediaries

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 $\rightarrow$ honest recording $\rightarrow$ no double-spending
    - ⋆ Biais, Bisiere, Bouvard, and Casamatta (2018)
  - Open access and trustless $\rightarrow$ little market power for intermediaries

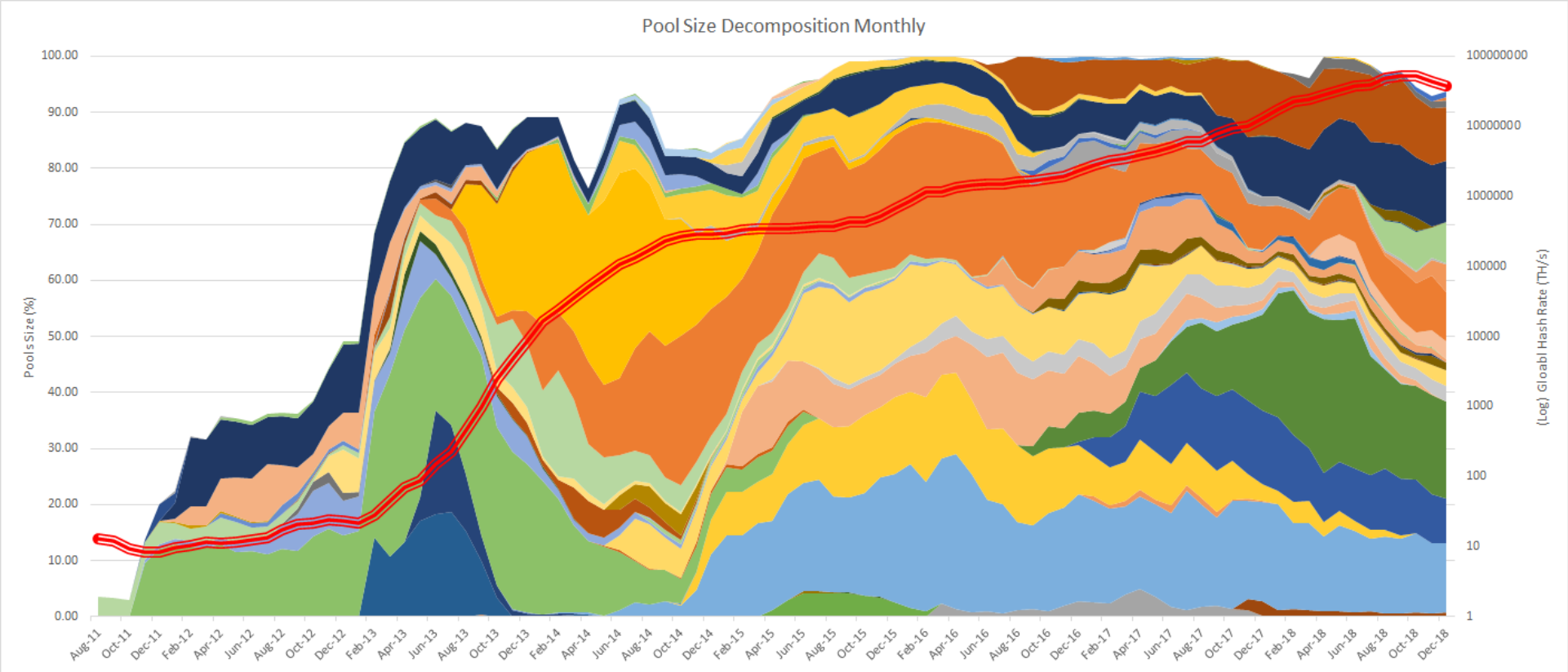
Decentralized Consensus: the Bitcoin Example

- 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 $\rightarrow$ honest recording $\rightarrow$ no double-spending
    - ⋆ Biais, Bisiere, Bouvard, and Casamatta (2018)
  - Open access and trustless $\rightarrow$ 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"
    - ⋆ Two examples: "mining war" during BCH forking; and mining pool evolutions
  - Concerns over sustainability (51% attack, selfish mining, etc.)
- We offer fresh economic analyses to
  - clarify certain fallacies
  - highlight one important mechanism linking "pools" and "rising mining power"

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

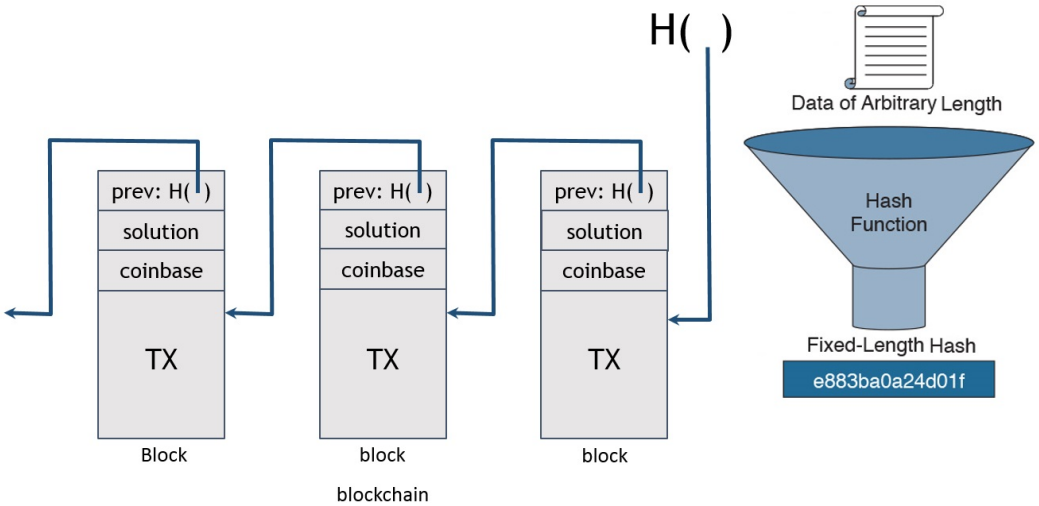
- Risk-aversion $\Longrightarrow$ pooling: significant risk-sharing benefits
  - Diversifying via pools improves (risk-averse) individual payoff but worsens the arms race of mining, quantitatively significant
  - **Links egregious energy use with pools**; financial innovation aggravates arms race (5$\sim$10 times)
- Risk-aversion $\Longrightarrow$ pools; but $\not\Longrightarrow$ pools to merge/centralization
  - Miners can join multiple pools, diversify by themselves
  - M&M: investors diversify themselves $\Longrightarrow$ 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
- 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
  - $\sim$1 block/10 mins; my mining hurts others' winning probability
  - The exact source of arms race (negative) externality



A live demo

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
- Λ: **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

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
- Λ: **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 λ_A who joins a (free) pool with Λ_B is

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

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

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 λ_A who joins a (free) pool with Λ_B is

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

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

Solo vs Pool

A miner with λ_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
- $R = \$100,000$ $((12.5+ \sim 0.5)BTC/\text{block} \times \$8\text{K/BTC} \Rightarrow \$104\text{K})$
- CARA $\rho = .00002$ (CRRA of 2 / wealth of \$100K)
- $T = 3600 \times 24\text{s}$: 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

Caveat: miners are deciding how to allocate across pools, not whether or not join pools

Mining Pool: Structure and Fee Contract

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**
  - Hash(**partial solution**, 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

$\sim$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 $r = \frac{RT}{D\Lambda}(1-f_{PPS})$
   - hourly-based wage
3. cloud mining: exactly the opposite of PPS

We focus on proportional pools

- $\sim$70% of pools adopt (28% exclusively)
- PPS/cloud only relevant for heterogeneous risk aversions

Evolution of Pool Sizes and Fee Contracts

Year	Hash Rate (PH/s) (A)	# of Pools (B)	% of Top 5 (C)	Avg. Fee (%), Size-weighted (D)	Frac. (%) Pools w. Prop. Fee (E)	Fee (%)			
						Top 5		All	
						Prop. (F)	Ave. (G)	Prop. (H)	Ave. (I)
2011	0.01	7	7.63	0.72	85.98	0.28	0.28	0.28	0.25
2012	0.02	15	34.66	2.69	60.03	0.66	1.76	0.65	1.56
2013	1.48	23	71.01	2.73	61.20	1.58	2.29	1.16	2.02
2014	140.78	33	70.39	0.94	73.19	1.33	1.13	0.88	2.38
2015	403.61	43	69.67	1.73	81.97	1.10	1.31	0.84	1.33
2016	1,523.83	36	75.09	2.60	78.74	1.48	2.15	0.97	1.67
2017	6,374.34	43	62.25	1.44	89.85	2.00	1.43	1.45	1.33
2018	36,384.60	40	69.15	1.31	70.24	1.08	1.62	0.99	1.47

Current Contract Sample

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

Outline

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

Model Setup

- Static game, CARA $u(x) = \frac{1}{\rho}\left(1 - e^{-\rho x}\right)$
- N measure of active miners acquire hash rate λ_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
- Analyzing the baseline model first, then add the following "Friction"
- Pool m endowed with passive hash rates $\Lambda_{pm} \geq 0$
  - "Loyal fans," proprietary hash power (mining factory), etc.
  - Key to **monopolistic competition**
    - Monopolistic competition: *a type of imperfect competition; producers sell differentiated products (e.g. branding or quality) that are not perfect substitutes*
  - Empirical link to initial pool size

Model Setup

- Static game, CARA $u(x) = \frac{1}{\rho}\left(1 - e^{-\rho x}\right)$
- N measure of active miners acquire hash rate λ_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
- Analyzing the baseline model first, then add the following "Friction"
- Pool m endowed with passive hash rates $\Lambda_{pm} \geq 0$
  - "Loyal fans," proprietary hash power (mining factory), etc.
  - Key to **monopolistic competition**
    - ★ Monopolistic competition: *a type of imperfect competition; producers sell differentiated products (e.g. branding or quality) that are not perfect substitutes*
  - Empirical link to initial pool size

Active Miner's Problem

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

the problem reduces to

$$\max_{\lambda_m \geq 0}\left[\frac{\Lambda_{am}+\Lambda_{pm}}{\rho\Lambda}\left(1-e^{-\frac{\rho R(1-f_m)\lambda_m}{\Lambda_{am}+\Lambda_{pm}}}\right) - C\lambda_m\right], \forall m, \tag{2}$$

where the global hash rate Λ is

$$\Lambda = \sum_{m=1}^{M}(\Lambda_{am}+\Lambda_{pm}). \tag{3}$$

Active Miner's Problem

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

the problem reduces to

$$\max_{\lambda_m \geq 0}\left[\frac{\Lambda_{am}+\Lambda_{pm}}{\rho\Lambda}\left(1-e^{-\frac{\rho R(1-f_m)\lambda_m}{\Lambda_{am}+\Lambda_{pm}}}\right) - C\lambda_m\right], \forall m, \tag{2}$$

where the global hash rate Λ is

$$\Lambda = \sum_{m=1}^{M}(\Lambda_{am}+\Lambda_{pm}). \tag{3}$$

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

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

- Each managers takes into account the effect of his own fees f_m on global hash rates Λ
- .....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

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

- Each managers takes into account the effect of his own fees f_m on global hash rates Λ
- .....infinitesimal miners do not

Equilibrium Definition

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 $\Longrightarrow$ pools merge/centralization"
- An interesting forum post (after we wrote the paper):
  - *Mining in multiple pools not only helps variance for individual miners, but is healthier for the network. In the current standard usage, there is a 'the rich get richer, the poor get poorer' tendency where larger pools are more attractive and thus grow even larger..... If miners adopt the proposed strategy, the tendency will be to maintain the status quo distribution, so pools can rise and fall based on their merits. Miners will enjoy the low variance of a single huge pool, without the centralization of power problem.*

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 $\Longrightarrow$ pools merge/centralization"
- An interesting forum post (after we wrote the paper):
  - *Mining in multiple pools not only helps variance for individual miners, but is healthier for the network. In the current standard usage, there is a 'the rich get richer, the poor get poorer' tendency where larger pools are more attractive and thus grow even larger..... If miners adopt the proposed strategy, the tendency will be to maintain the status quo distribution, so pools can rise and fall based on their merits. Miners will enjoy the low variance of a single huge pool, without the centralization of power problem.*

The Dark Side of Risk-Sharing of Mining Pools

- **Mining arms race**

- In our simplified Economic modeling, any miner will (honestly) record transaction, and energy in mining competition is just a waste
  - PoW protocol has other benefits not captured by this model
  - Say, security
  - Interesting/challenging to incorporate this feature into this framework

- 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:

$$\underbrace{\frac{R(1-f_m)}{\Lambda}}_{\text{risk-neutral valuation}} \underbrace{e^{-\rho R(1-f_m)\frac{\lambda_m}{\Lambda_{am}+\Lambda_{pm}}}}_{\text{risk aversion discount}} = \underbrace{C}_{\text{marginal cost}} . \tag{5}$$

- Larger (better diversified) pools attract more allocation
- Marginal benefit of very first unit ($\lambda_m = 0$) is risk-neutral valuation (only the 1st term remains)
  - Any pool will attract some active miners in equilibrium
  - Analogy: heterogenous producers (pools) engaging in Like **monopolistic competition** who serve consumers (active miners)

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

$$\frac{\lambda_m}{\Lambda_{pm}} = \frac{\ln \frac{R(1-f_m)}{C\Lambda}}{\rho R(1-f_m) - N \ln \frac{R(1-f_m)}{C\Lambda}} \tag{6}$$

Equilibrium with Passive Hash Rates

Active miner's FOC:

$$\underbrace{\frac{R(1-f_m)}{\Lambda}}_{\text{risk-neutral valuation}} \underbrace{e^{-\rho R(1-f_m)\frac{\lambda_m}{\Lambda_{am}+\Lambda_{pm}}}}_{\text{risk aversion discount}} = \underbrace{C}_{\text{marginal cost}} . \tag{5}$$

- Larger (better diversified) pools attract more allocation
- Marginal benefit of very first unit ($\lambda_m = 0$) is risk-neutral valuation (only the 1st term remains)
  - Any pool will attract some active miners in equilibrium
  - Analogy: heterogenous producers (pools) engaging in Like **monopolistic competition** who serve consumers (active miners)

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

$$\frac{\lambda_m}{\Lambda_{pm}} = \frac{\ln \frac{R(1-f_m)}{C\Lambda}}{\rho R(1-f_m) - N \ln \frac{R(1-f_m)}{C\Lambda}} \tag{6}$$

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
     $\Longrightarrow$ 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

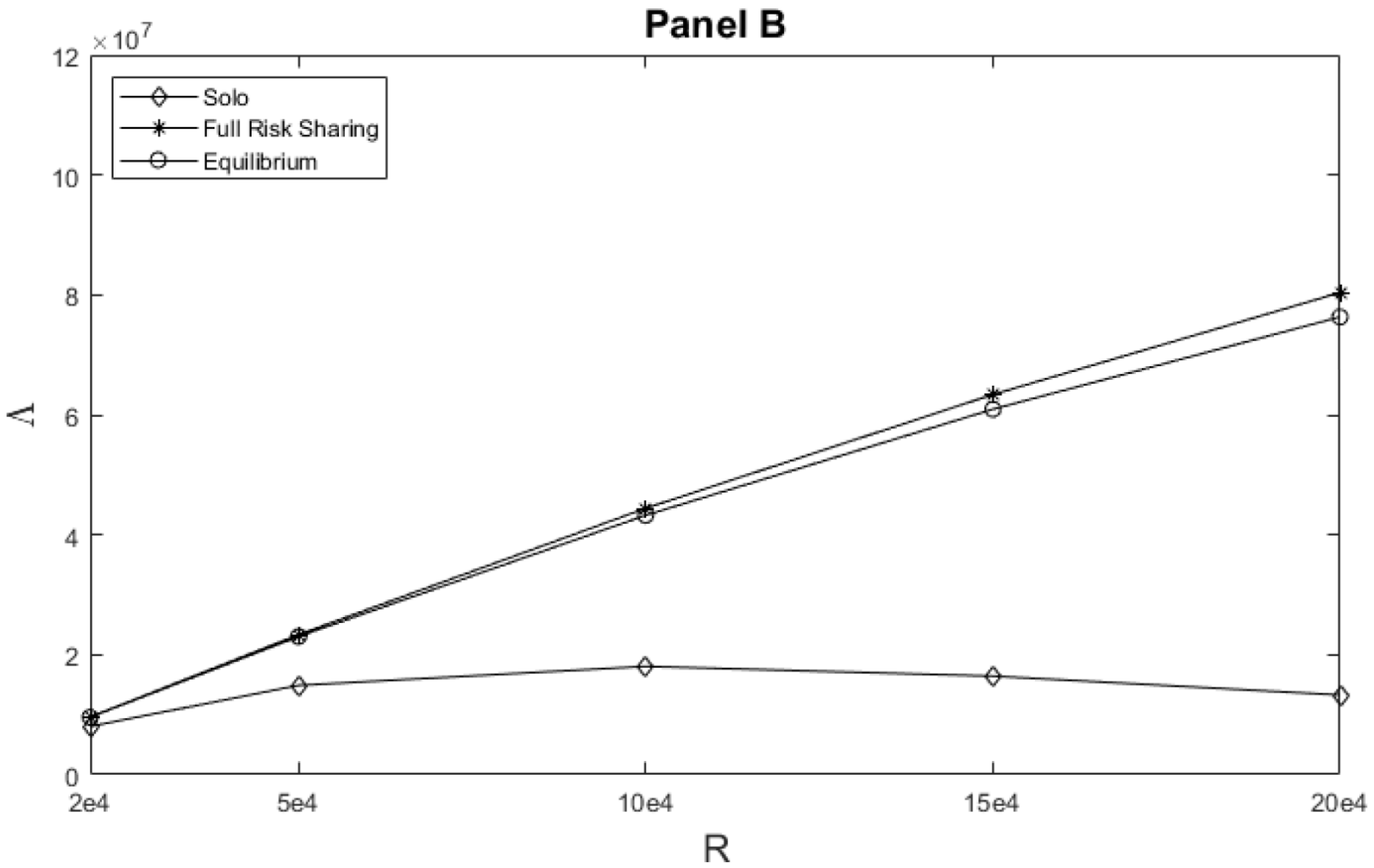
Same fee, same growth; higher fee, lower growth.

- *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

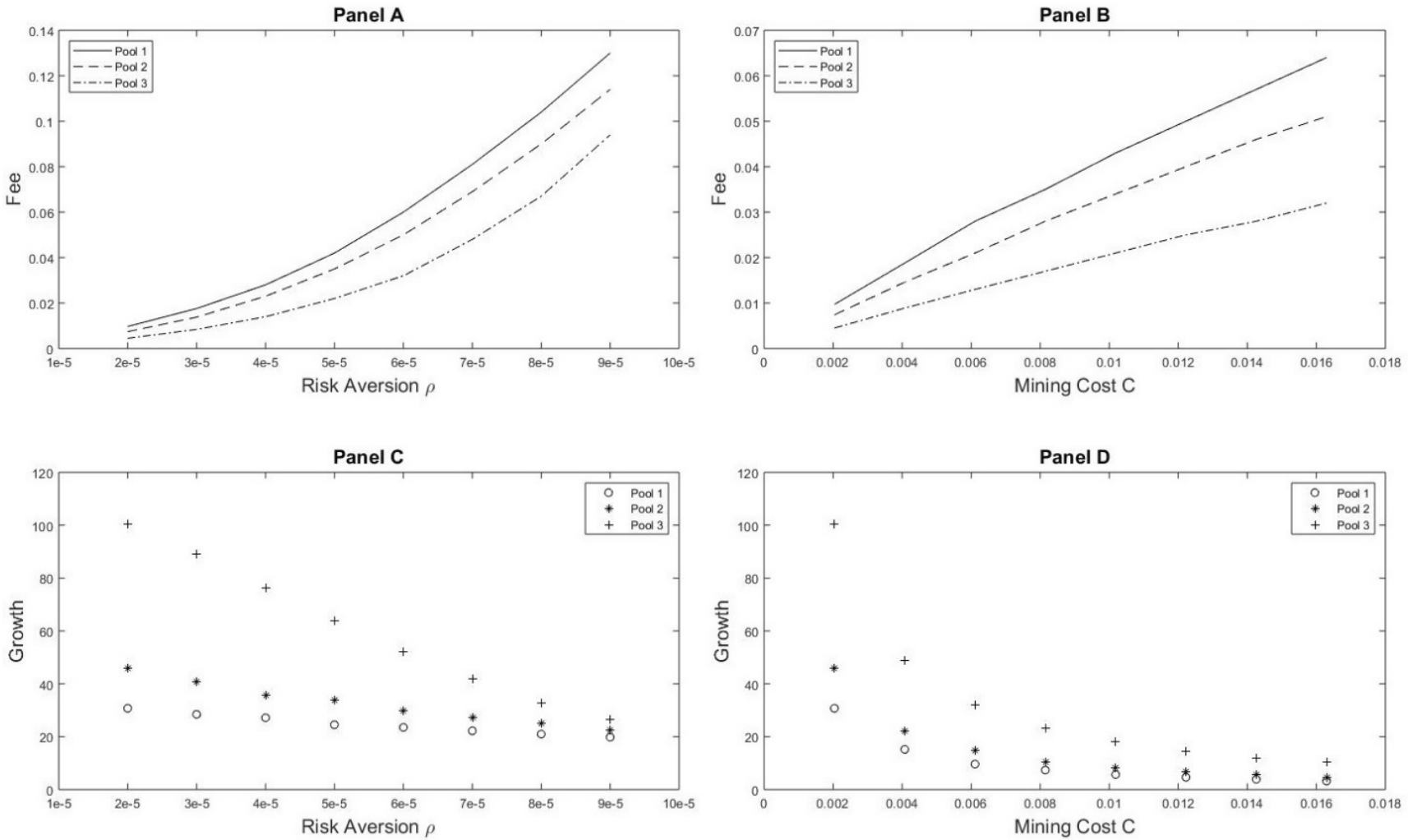
1. **Social cost of pools**
   - Equilibrium of symmetric pools ($\Lambda_{pm} = \Lambda_p$)
   - Oligopolistic pools take arms race into account, charge positive fees
     $\Longrightarrow$ less global hash rates than full risk-sharing but more than solo
2. What if heterogeneous pools: Larger pools charge higher fees?
   - Yes, because larger pools take into account of arms race effect more

Social Cost of Mining Pools



$R = 1 \times 10^5$, $N = 10$, $M = 2$, $C = 0.00204$, and $\rho = 1 \times 10^{-5}$.

Pool Evolution: Larger Λ_{pm}, Lower $\frac{\Lambda_{am}}{\Lambda_{pm}}$



$R = 1 \times 10^5$, $\lambda_a = 5 \times 10^4$, $N = 10$, $\Lambda_{p1} = 5 \times 10^5$, $\Lambda_{p2} = 3 \times 10^5$, $\Lambda_{p3} = 1 \times 10^5$, $C = 0.00204$, 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 (monthly)
- the newly mined blocks divided by total blocks mined globally (a widely used estimator)

Data on pool fee/reward type evolution

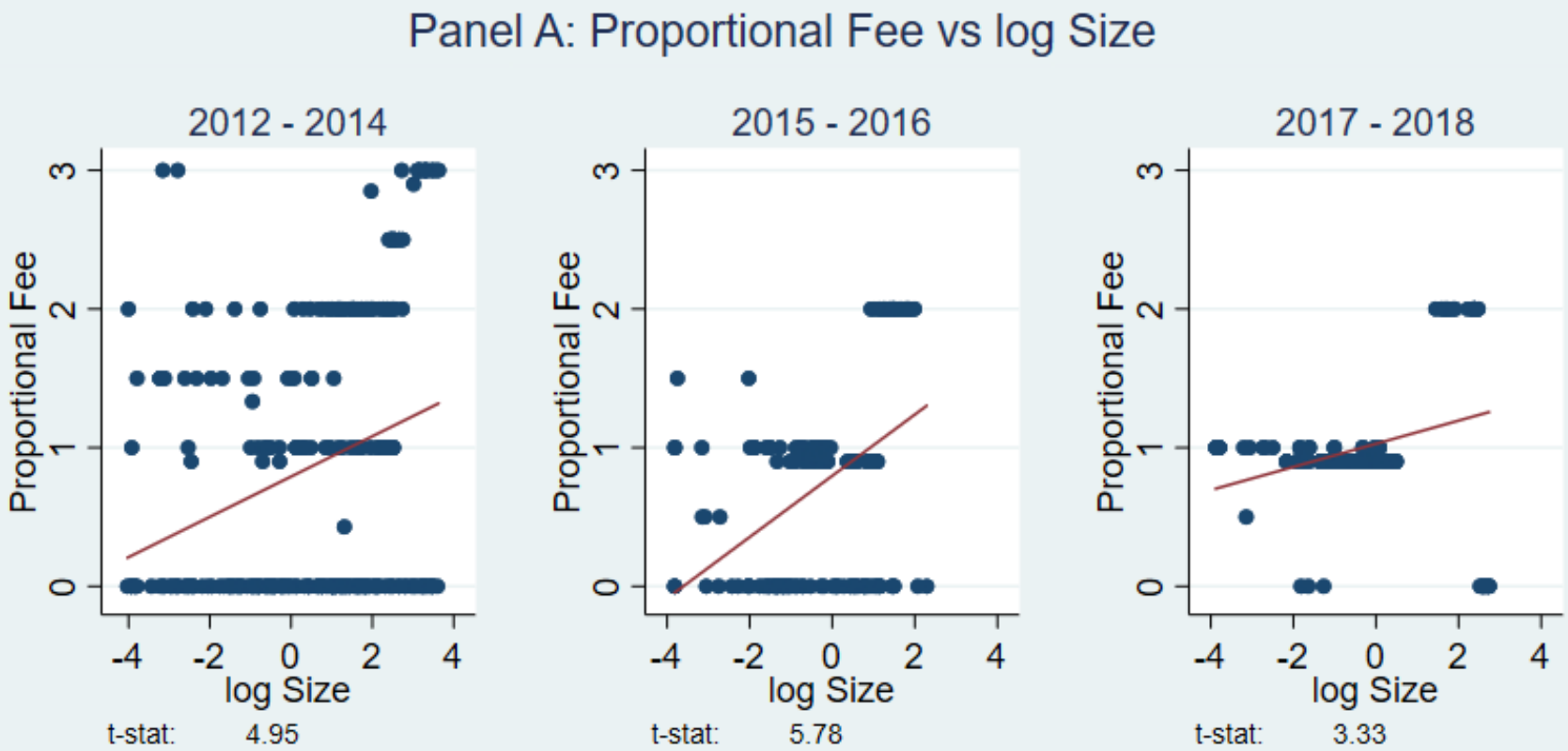
- Bitcoin Wiki: Comparison of mining pools
- the entire Wiki revision history

What we do

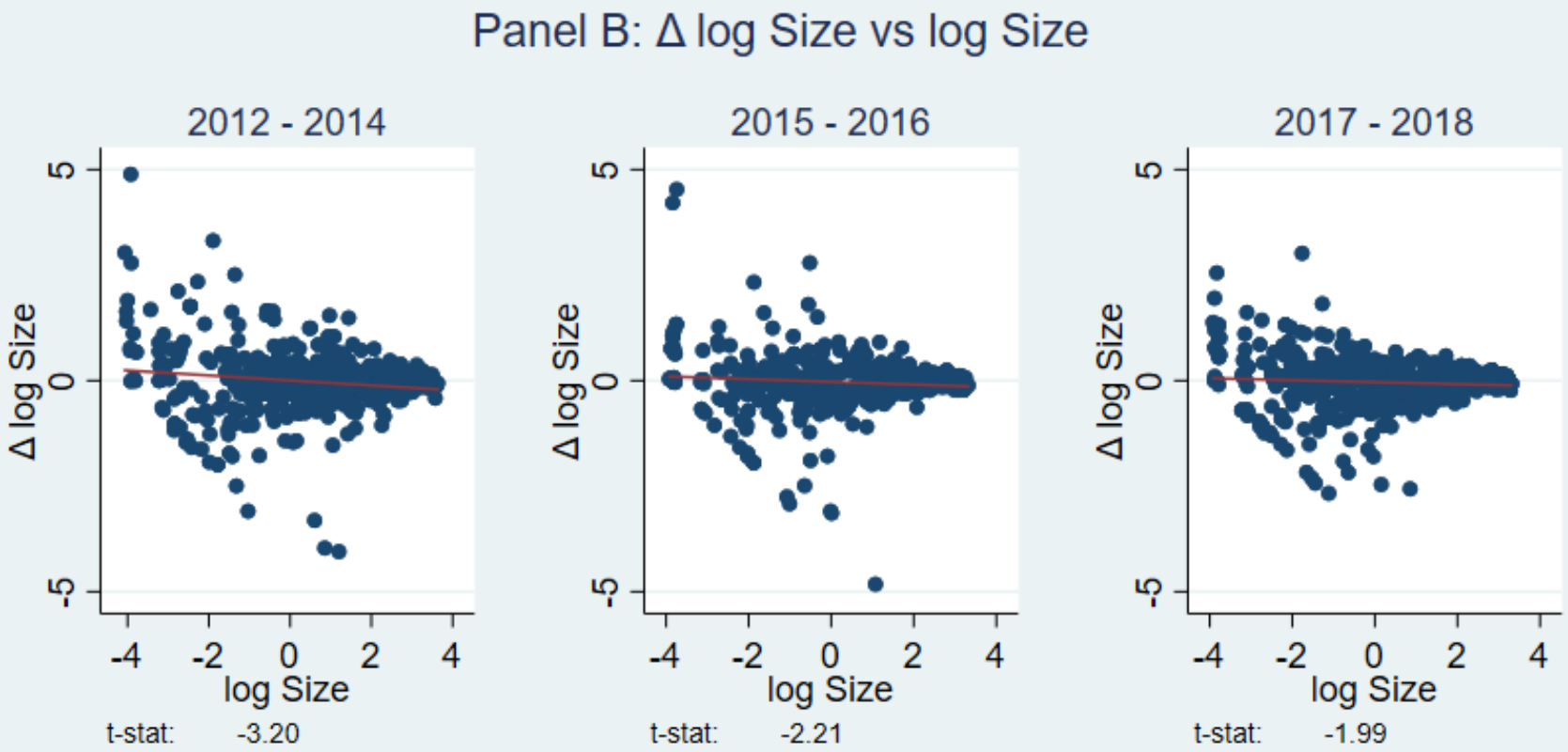
1. investigate relationships between monthly growth rates /average fees and previous month hashrate share in three windows

   (i.e., 2012-2014, 2015-2016, and 2017-2018)

Empirical Evidence: Results



Empirical Evidence: Results



Pool Size, Fee, and Growth: Regression Results

	Panel A: *Proportional Fee*			
	2012-2014	2015-2016	2017-2018	2012-2018
	(1)	(2)	(3)	(4)
logSize	0.16***	0.24***	0.09***	0.16***
	(4.95)	(8.63)	(4.18)	(7.67)
Adjusted R^2	-0.007	0.078	-0.052	-0.002
Month FE	Yes	Yes	Yes	Yes
Observations	286	147	140	573

	Panel B: Δ*logSize*			
	2012-2014	2015-2016	2017-2018	2012-2018
log *Size*	-0.05**	-0.03*	-0.02	-0.03***
	(-2.35)	(-1.90)	(-1.36)	(-3.23)
Adjusted R^2	0.013	-0.004	0.031	0.016
Month FE	Yes	Yes	Yes	Yes
Observations	499	562	644	1705

t statistics in parentheses

$^{*}: p < 0.10, ^{*}* : p < 0.05, ^{*}** : p < 0.01$

Measuring Passive Sizes

1. Identify pool manager addresses from coinbase transactions
   - label all transactions sent from pool manager addresses as paychecks
2. Within each pool, define
   - loyalty addresses: ones having only appeared in a unique pool manager's paychecks
   - seed addresses: top 10 addresses receiving the most bitcoins from the pool manager within a month
   - relationship addresses: top 10% addresses receiving the most bitcoins from the pool manager within a month
3. A pool's loyalty (seed, relationship) size: scale by global hashrates

Loyalty, seed, and relationship sizes are noisy proxies for passive size

Passive Size, Pool Fee, and Growth: Regression Results

	Panel A: *Proportional Fee*			
	log Pool Size (1)	log Loyalty Size (2)	log Seed Size (3)	log Relationship Size (4)
Coefficient	0.16***	0.12***	0.17***	0.20***
t statistics	(7.67)	(8.17)	(6.23)	(10.19)
Adjusted R^2	-0.002	-0.077	-0.096	0.013
Monthly FE	Yes	Yes	Yes	Yes
# Obs.	573	396	413	413
	Panel B: $\Delta logSize$ or $\Delta Active\_Growth$			
Coefficient	-0.03***	-9.73***	-0.36***	-0.34***
t statistics	(-3.23)	(-20.49)	(-11.66)	(-16.21)
Adjusted R^2	0.016	0.429	0.128	0.170
Monthly FE	Yes	Yes	Yes	Yes
# Obs.	1705	1154	1287	1287

t statistics in parentheses

*: $p < 0.10$, **: $p < 0.05$, ***: $p < 0.01$

Outline

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

Entry and Market Power

- M^I incumbents; entrants incur $K \geq 0$ to enter.
  - also: secure passive hash rates for an additional cost $K' > 0$

Proposition (Market Power of Incumbent Pools)

Incumbent pools ($\Lambda_{pm} > 0$) always charge $f_m > 0$ and attract $\Lambda_{am} > 0$.

  - This is true even for $K = 0$ (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 (ϵ 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 $\Longrightarrow$ pools, but diversification across pools sustains decentralization
   - MM insight, IO insight $\rightarrow$ 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