Monopoly without a Monopolist: Economics of the Bitcoin Payment System

Gur Huberman, Jacob D. Leshno, Ciamac Moallemi
Columbia Business School

Cryptocurrencies

- Electronic payment systems
  - Bitcoin being the first
  - More than 10 systems have total balances of over $1B
  - New systems developed, offering new functionality
- Decentralized, two-sided markets
  - Users receive similar services to PayPal, Fedwire; Miners provide infrastructure
  - Market design enabled by blockchain protocol
- Novel economic structure
  - Owned by no one
  - Rules fixed by a computer protocol
  - All (small) agents are price-takers

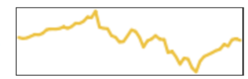
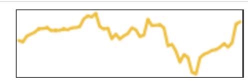
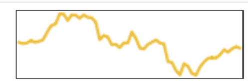
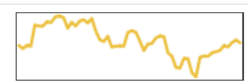
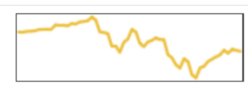
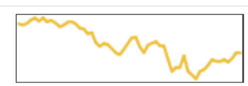
Cryptocurrencies

868 Currencies / 236 Assets / 5474 Markets Market Cap: $159,773,994,232 / 24h Vol: $6,528,166,064 / BTC Dominance: 47.1%

CryptoCurrency Market Capitalizations

Market Cap ▾ Trade Volume ▾ Trending ▾ Tools ▾ Search Currencies

All ▾ Currencies ▾ Assets ▾ USD ▾ Next 100 → View All

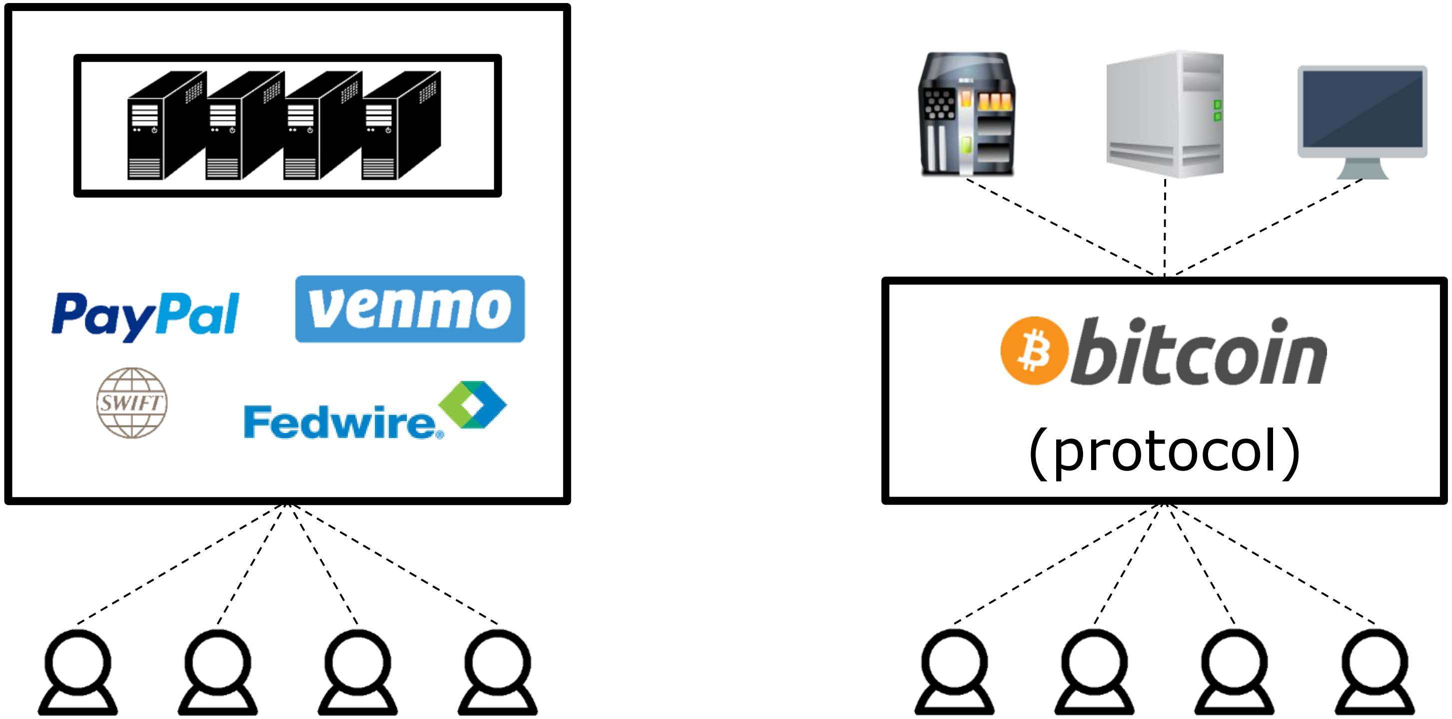
#	Name	Market Cap	Price	Circulating Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	Bitcoin	$75,219,057,588	$4545.48	16,548,100 BTC	$2,281,740,000	6.46%	
2	Ethereum	$30,734,261,898	$325.36	94,463,195 ETH	$1,197,820,000	8.02%	
3	Bitcoin Cash	$10,615,945,842	$640.94	16,563,063 BCH	$586,182,000	21.33%	
4	Ripple	$8,465,783,474	$0.220786	38,343,841,883 XRP *	$174,811,000	4.79%	
5	Litecoin	$3,984,112,940	$75.45	52,807,757 LTC	$787,911,000	10.99%	
6	NEM	$2,693,916,000	$0.299324	8,999,999,999 XEM *	$5,256,710	7.32%	
7	Dash	$2,518,908,128	$334.01	7,541,348 DASH	$38,438,700	6.03%	
8	IOTA	$1,873,734,175	$0.674119	2,779,530,283 MIOTA *	$31,955,200	13.86%	

Source: https://coinmarketcap.com/ (accessed 9/6/2017)

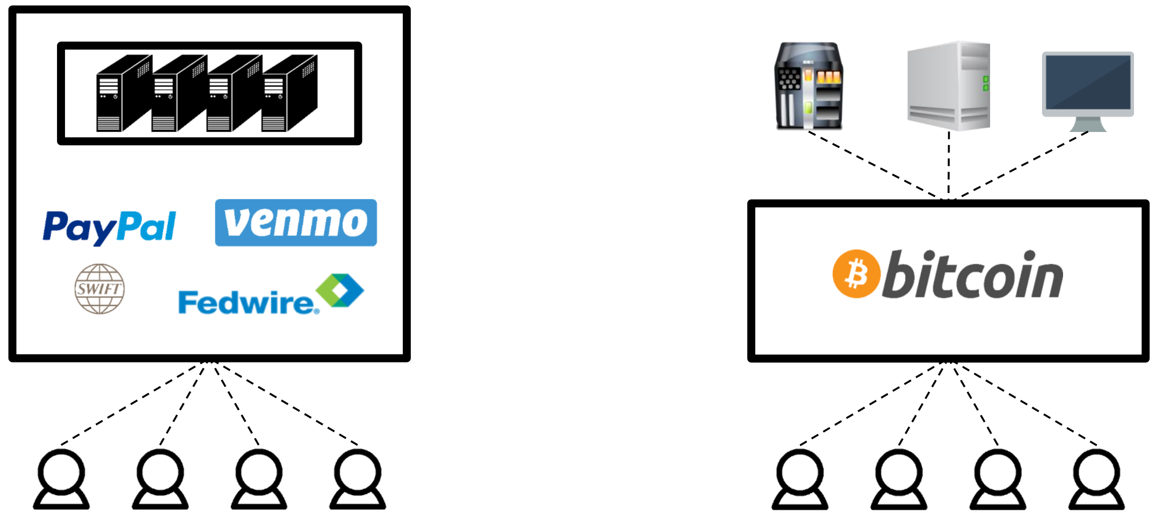
Traditional Electronic Payment Systems

- Allows users to hold balances and make transfers
- Controlling authority
  - Provide trust, maintain infrastructure, sets usage fees
- Natural monopoly
  - Network externalities, fixed costs
  - Often requires regulation
- Examples: Fedwire, Venmo, PayPal, SWIFT, M-Pesa

Traditional Payment Systems vs. Bitcoin

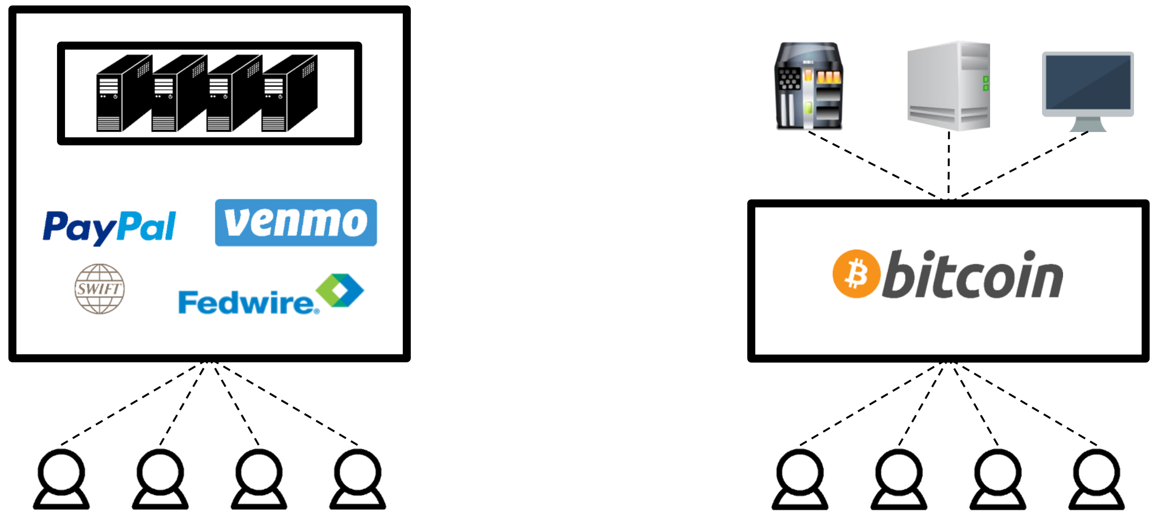


Traditional Payment Systems vs. Bitcoin



Rules	Set by firm/org	Fixed by protocol
Infrastructure	Procured by firm/org	
Revenue	Fees set by firm/org	

Traditional Payment Systems vs. Bitcoin



Rules	Set by firm/org	Fixed by protocol
Infrastructure	Procured by firm/org	*Revenue, entry/exit*
Revenue	Fees set by firm/org	*Equilibrium congestion pricing, all agents served*

Related Literature

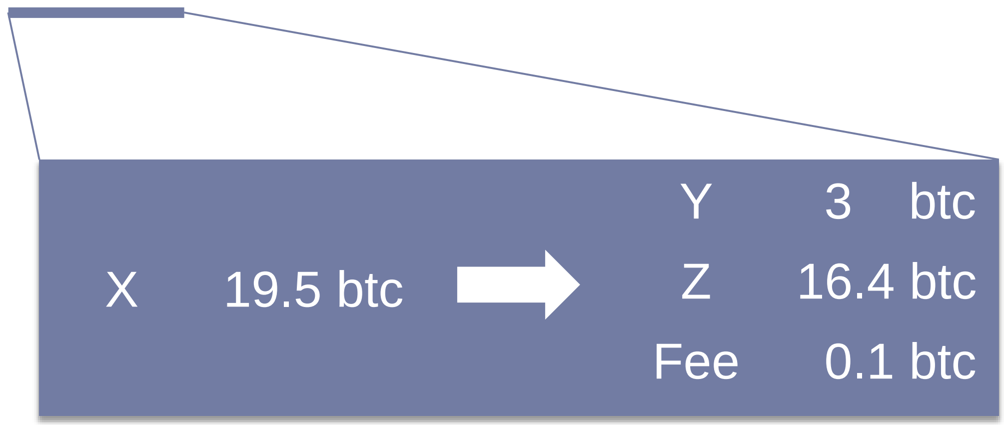
- Blockchain
  - Nakamoto (2008), Eyal & Sirer (2014), Sapirshtein et al. (2016), Narayan et al. (2016), Carlsten et al. (2016) Chiu & Koeppl (2017), Easley et al. (2017), Kroll et al. (2013)
- Usage of Bitcoin and the cryptocurrency market
  - Ron & Shamir (2013), Athey et al. (2016), Yermack (2013)
  - Gandal & Halaburda (2014), Halaburda & Sarvary (2016), Gans & Halaburda (2015), Catalini & Gans (2016), Cong & He (2017)
- Queueing theory
  - Lui (1985), Glazer & Hassin (1986), Hassin (1995), Hassin & Haviv (2003)

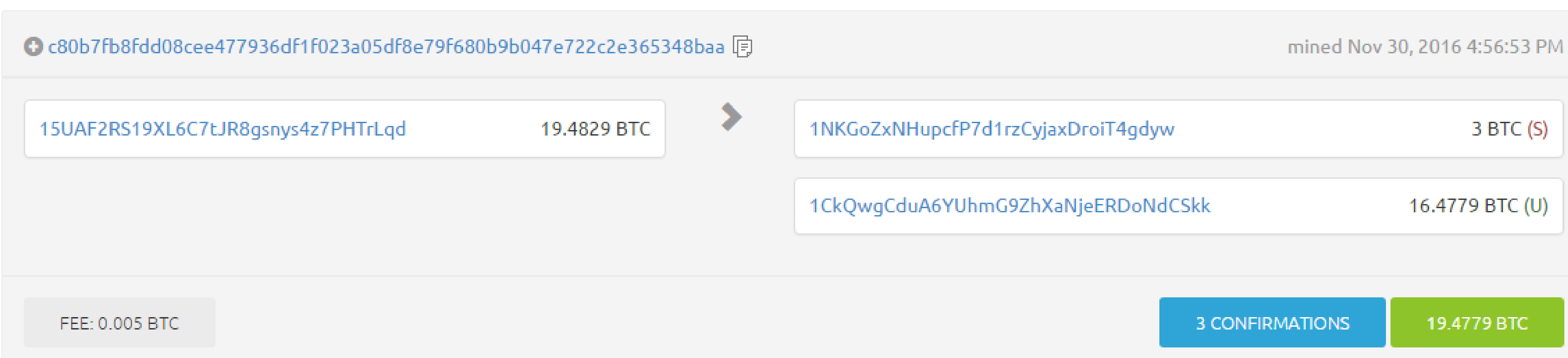
Talk outline

- Background – the Blockchain protocol
  - "Blockchain for economists"
- Economic model of Bitcoin as a two-sided platform
  - Analytical solutions
  - Empirical evidence
- Implications and design considerations

The Blockchain ledger

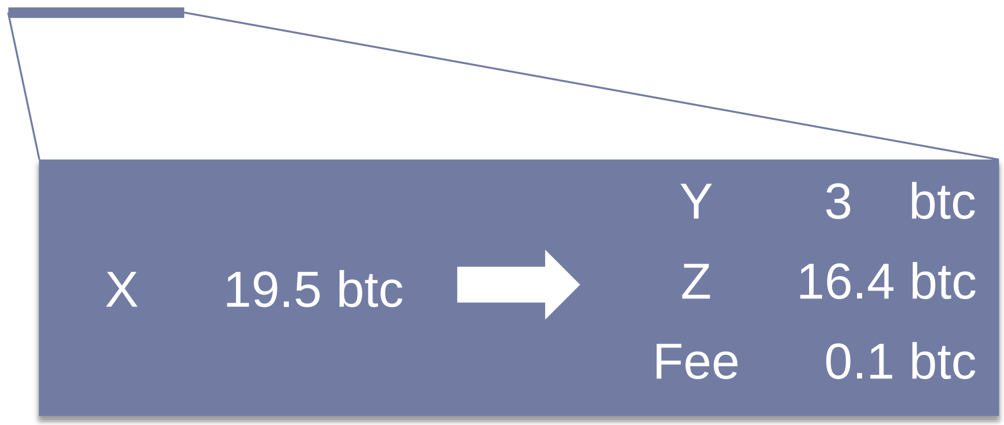
- A bitcoin transaction is a balance transfer between addresses
- Sent publicly (to the mempool)





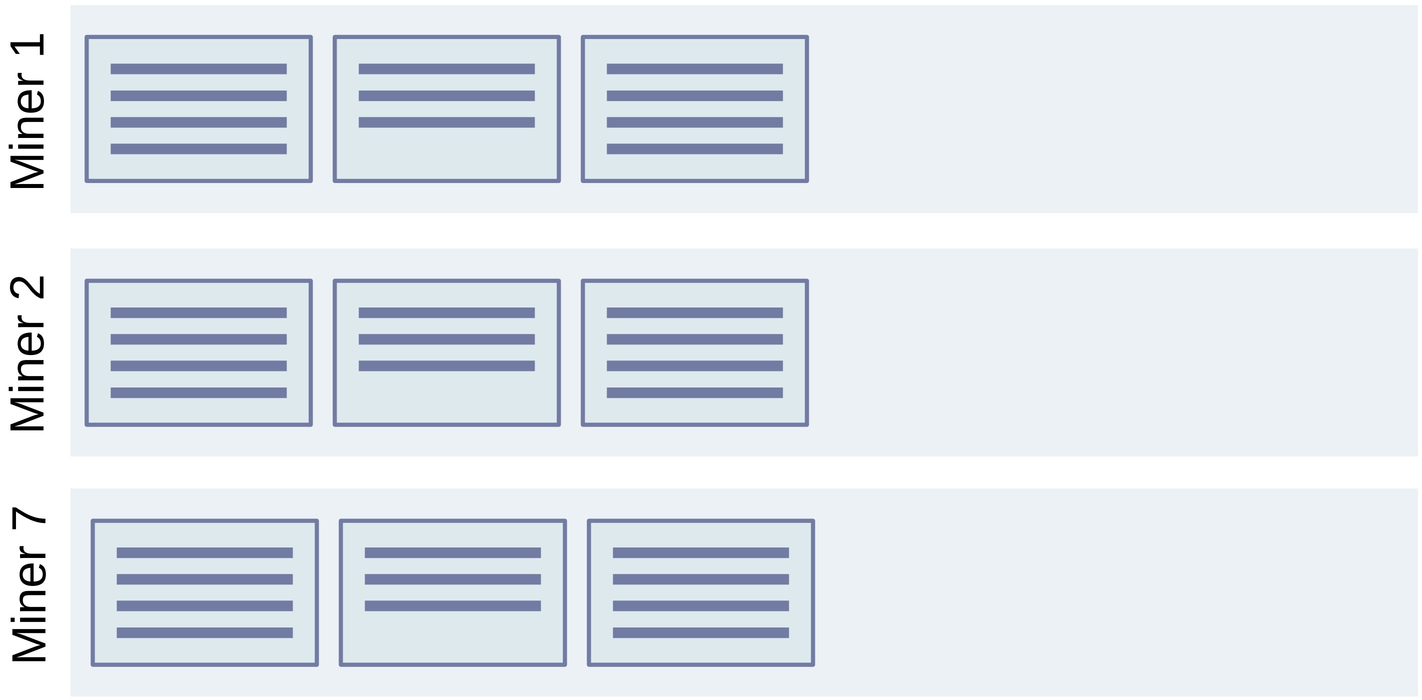
The Blockchain ledger

- A bitcoin transaction is a balance transfer between addresses



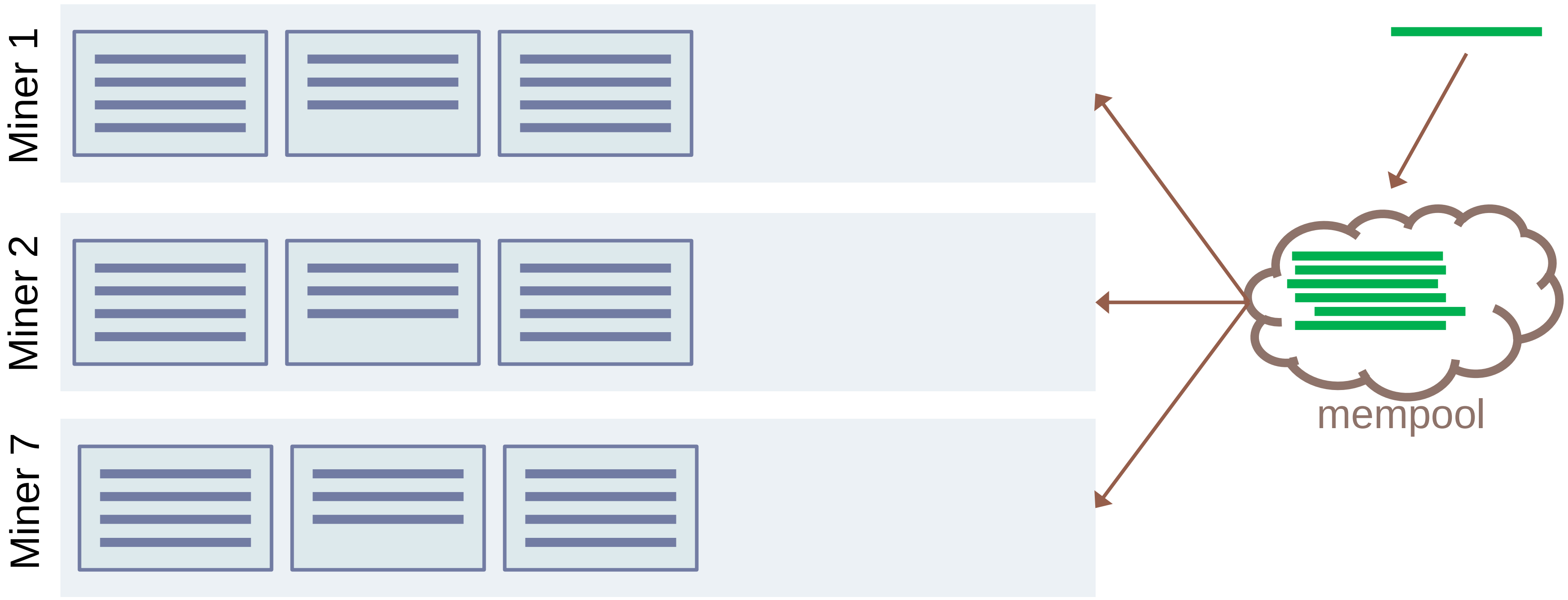
- The Blockchain ledger is a list of all past transactions, organized into blocks

Blockchain



- Many Miners, free entry
- All hold identical copies of the blockchain

Blockchain

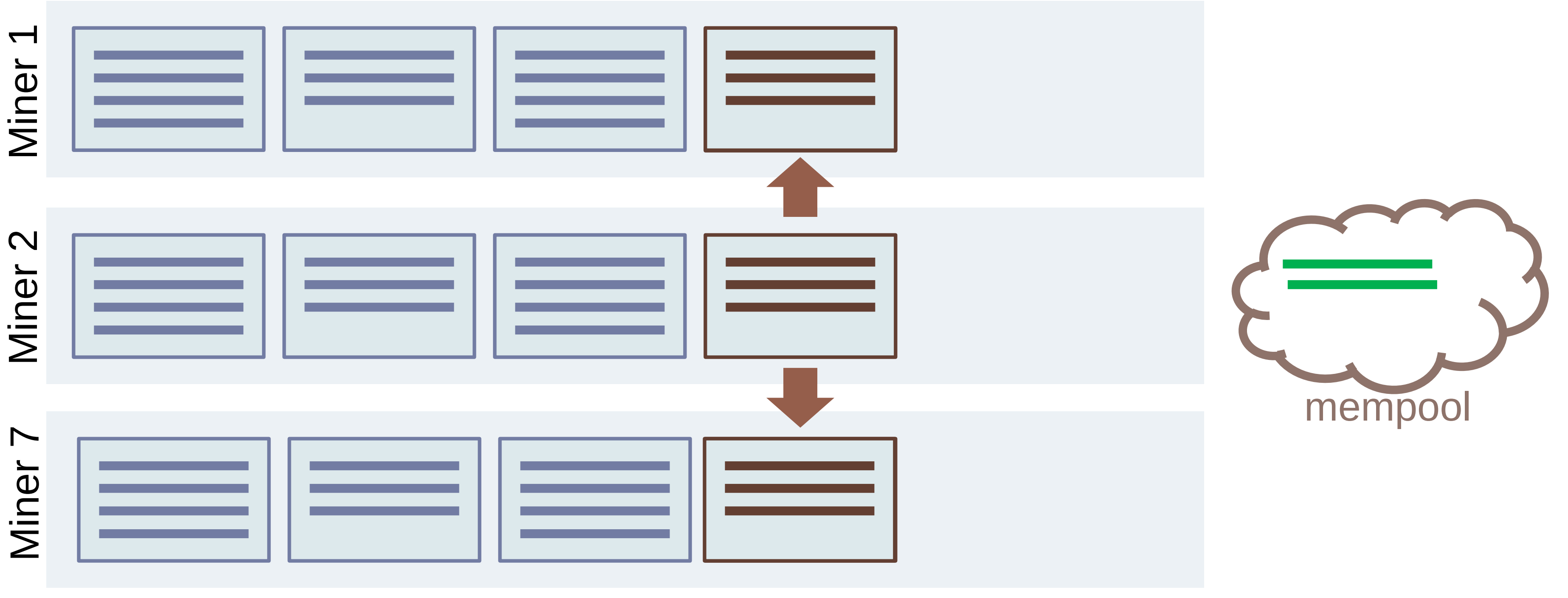


- New transactions transmitted to all miners

Blockchain

- Every 10 min (on avg), one randomly selected miner creates/mines a new block
- Maximal block size is 1MB (approx. 2000 transactions)
  - Unprocessed transactions remain, wait for next block

Blockchain



- New mined block transmitted to all miners
- Vetted by others, becomes part of the blockchain

Blockchain

Blockchain

- Miners rewarded when mine a block:
  1. Fixed amount of newly minted coins
     - Majority of current reward
     - Only short term, halved every 4 years
  2. Transactions fees from transactions within the mined block
     - Long term

- Decentralized random selection by a tournament
  - Avoids the need for a trusted randomization device
  - Requires costly effort from each miner
  - Arrival of new blocks follows a Poisson process

Blockchain

- Equilibrium for (small) miners to follow the consensus blockchain
(Nakamoto 2008, Eyal & Sirer 2013)
  - Only valid transactions – verification using cryptography
  - Accept other's blocks – follow the longest chain
  - With sufficiently many miners the system is secure

Blockchain – Properties

- Users choose transaction fees
- (Small) Miners are price takers
  - Provide computational infrastructure, rewarded by transaction fees and newly minted coins
  - Cannot block transactions, affect user behavior or transaction fees
- Free entry and exit of miners
- System's throughput independent of number of miners
  - Set by protocol parameters ($1MB$, 10min)

Simplified Economic Model

- N (small) miners
  - Equal computing power, equal cost of mining c_m
  - Many potential miners, free entry/exit
- Blocks mined at Poisson rate μ
  - Up to K transactions processed per block
- Users/transactions arrive at Poisson rate $\lambda < K \cdot \mu$
  - Each user has a single transaction, selects fee $b \geq 0$
  - Heterogeneous delay cost $c \sim F[\,0, \bar{c}\,]$

Simplified Economic Model

- Assumptions:
  - Unobservable queue
  - Sufficiently high value for service R, all users served
  - No new coins minted
  - Sufficiently many miners for the system to operate securely

Analysis of Miners

- In equilibrium, active miners maximize reward by procession K transactions with highest fees
  - Cannot affect the behavior of users or set transaction fees
  - Can observe pending transactions and their fees
  - Create block with highest fee transactions, up to block capacity

Analysis of Miners: Entry/Exit

- Total payment to miners is equal to total transaction fees
- Suppose Rev is total revenue (transaction fees) and there are N miners. Expected payment to each miner is

$$Rev/N$$

- Free entry/exit imply zero profit, implying the number of miners is

$$N = \frac{Rev}{c_m}$$

- Number of miners determined by Rev, c_m

Data: Cost per Transaction

	At max throughput 3.3 – 7 tx/sec	At real throughput 1.57 tx/sec
Mining: hashing	~$0.8 - $1.7	~$3.6
Mining: hardware (~annual cost)	~$0.6 - $1.3	~$2.7
Transaction validation	~$0.002	~$0.008
Bandwidth	~$0.02	~$0.08
Storage (running cost)	~$0.0008 / 5 years	

Source: Croman et.al (2016)

Data: Miners Costs and Revenue Oct 2015

Approx. total miners' cost (Croman et. al. 2016):

$$1.6\ {}^{tx}/_{sec} \cdot {}^{\$6}/_{tx} \cong \ \$10/\text{sec} = \ \$6{,}000/10\text{min}$$

- Approx. $325M annually

Approx. total reward:

$$25\ {}^{btc}/_{10\text{min}} \cdot {}^{\$300}/_{btc} = \ \$7{,}500/10\text{min}$$

- http://www.coinwarz.com/cryptocurrency

Analysis of Users/Transactions

- Users play a congestion queueing game
  - Blocks mined/added at rate μ, each processes K highest fee transactions
  - Transaction fees $b(c_i)$ are bids for priority
  - Independently of number of miners
- Equilibrium transaction fees $b_i = b(c_i)$ maximize

$$u(c_i) = \mathrm{R} - c_i \cdot W(b_i|G) - b_i$$

where $W(b_i|G)$ is the expected delay for a user who bids b_i given distribution of others bids G

Analysis of Users/Transactions

- Delay $W(b_i|G)$ depends only on
  - Arrival rate of higher priority transactions $\hat{\lambda}(b_i) = \lambda \cdot \bar{G}(b_i)$
  - Block size K, arrival rate μ
- In equilibrium $b(c_i)$ is increasing in c_i,
  - $\bar{G}(b_i) = \bar{F}(c_i)$
- Solving for the stochastic behavior of the system

$$W\left(b \mid G\right) = \mu^{-1} W_K\left(\rho \cdot \bar{F}\left(c_i\right)\right)$$

  - $\rho = \lambda/\mu K$ is a congestion parameter
  - $\hat{\rho} = \hat{\lambda}/\mu K = \rho\,\bar{F}(c_i)$ is effective congestion for c_i

Expected Wait Formulas

- Using generating functions, the expected wait of a transaction is

$$\mu^{-1} W_K(\hat{\rho}) = \frac{1}{\mu} \frac{1}{(1 - z_0)\left(1 + K\hat{\rho} + (K+1) z_0^K\right)}$$

where

- $\hat{\rho} = \hat{\lambda}/K\mu$, where $\hat{\lambda}$ is the arrival rate of higher priority transactions
- z_0 is the solution in $[0,1)$ of

$$z_0^{K+1} - (K\hat{\rho} + 1) z_0 + K\hat{\rho} = 0$$

Analysis of Users/Transactions

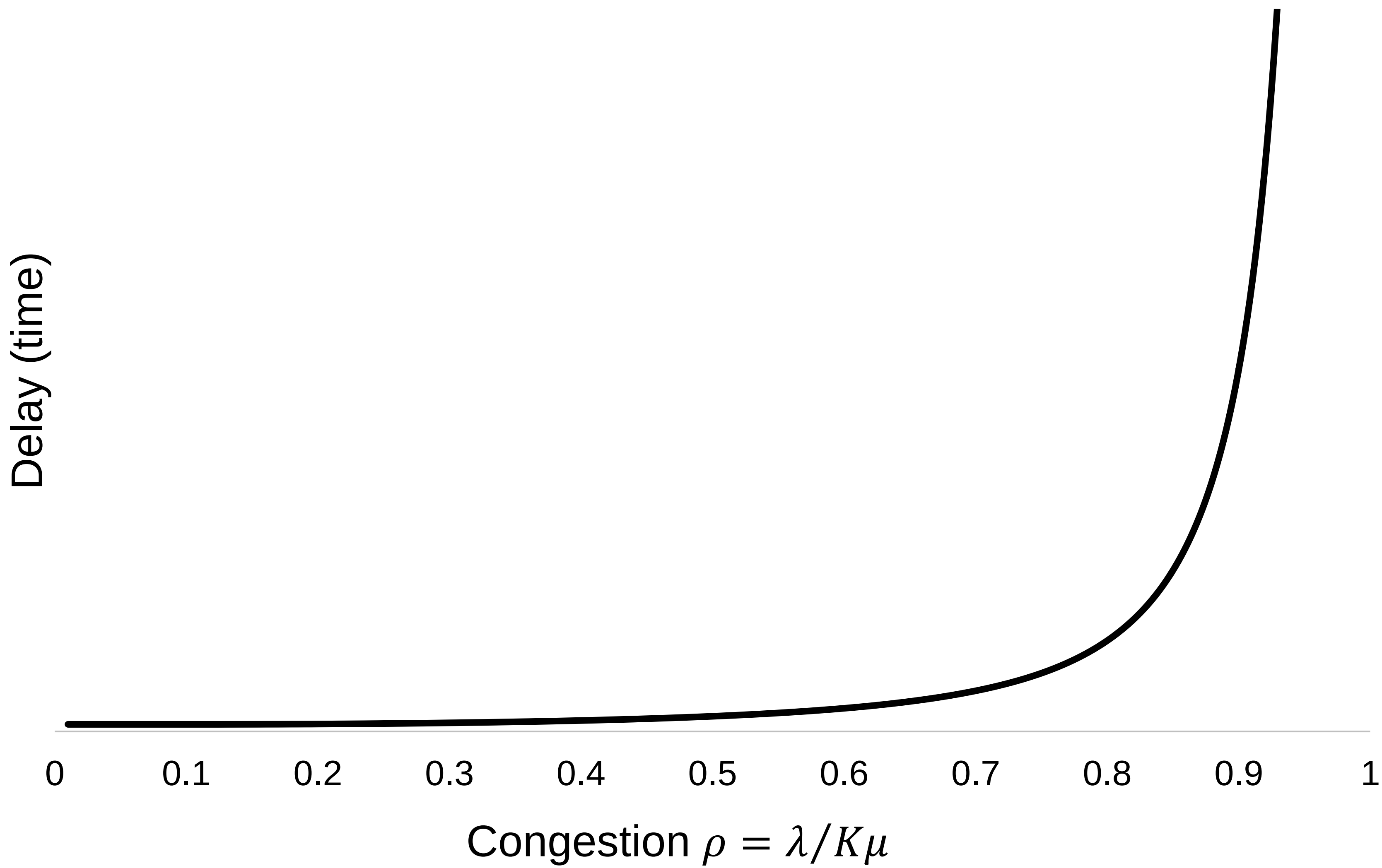
Lemma: In equilibrium,

- Users with higher delay costs pay higher transaction fees, receive higher priority and lower delay
- Transaction fee paid by a user is equal to the externality imposed on other transactions

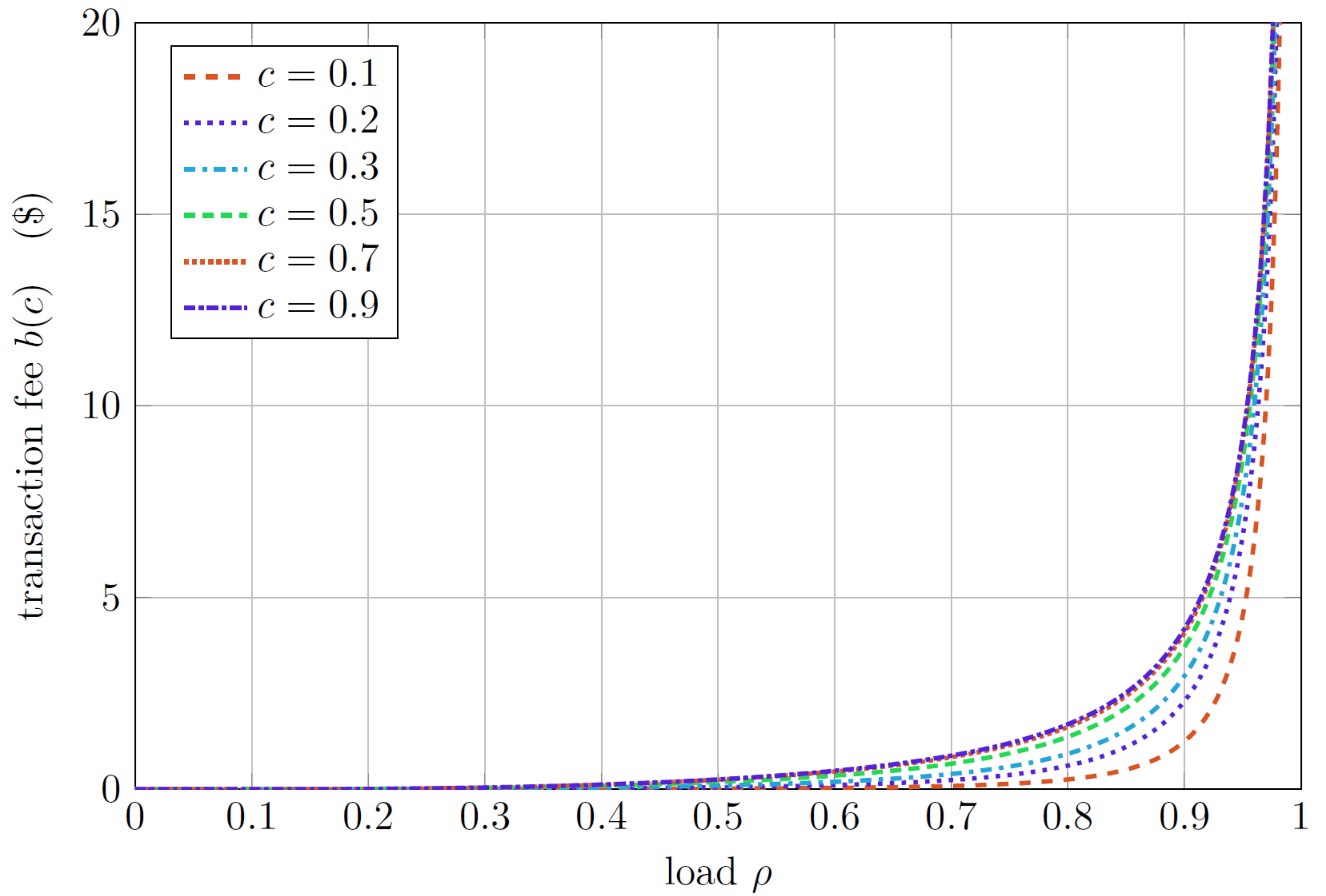
$$b(c_i) = \rho \int_0^{c_i} f(c) \cdot c \cdot \mu^{-1} W_K' \left(\rho \bar{F}(c) \right) dc$$

$$u(c_i) = R - \int_0^{c_i} \mu^{-1} W_K \left(\rho \bar{F}(c) \right) dc$$

Expected Delay for Lowest Priority Transaction given Congestion ρ

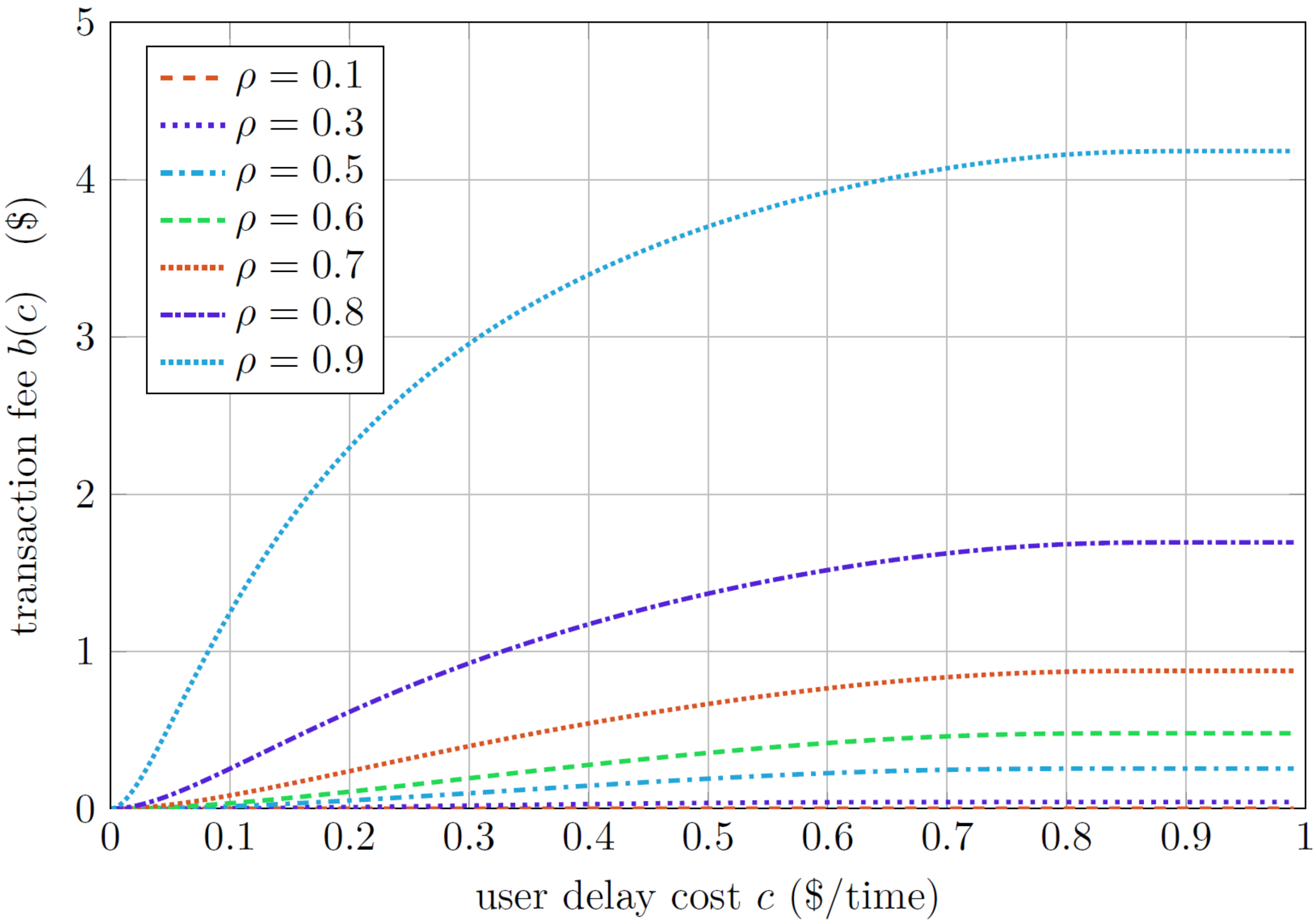


Equilibrium Transaction Fees as Function of Congestion



- Parameters: $K = 2{,}000$, delay costs distributed $c \sim U[0,1]$, $\mu = 1$

Equilibrium Transaction Fees as Function of User's Delay Cost



- Parameters: $K = 2{,}000$, delay costs distributed $c \sim U[0,1]$, $\mu = 1$

User Payments

- Positive payments, without excluding transactions
  - Strictly positive net reward to all users
  - Even transaction that pay no fee are processed
- No monopoly pricing, even if the system is a monopoly to users
- But payments and delays vary with congestion

- In contrast, a monopolist would:
  - Process all transactions without delay
  - Set a minimal fee
  - Exclude some users, or eliminate consumer surplus

Equilibrium Revenue and Delay Costs

Theorem: In equilibrium, revenue (total fees), delay costs and number of miners depend only on the distribution of delay cost F, congestion $\rho = \lambda/K\mu$ and block size K.

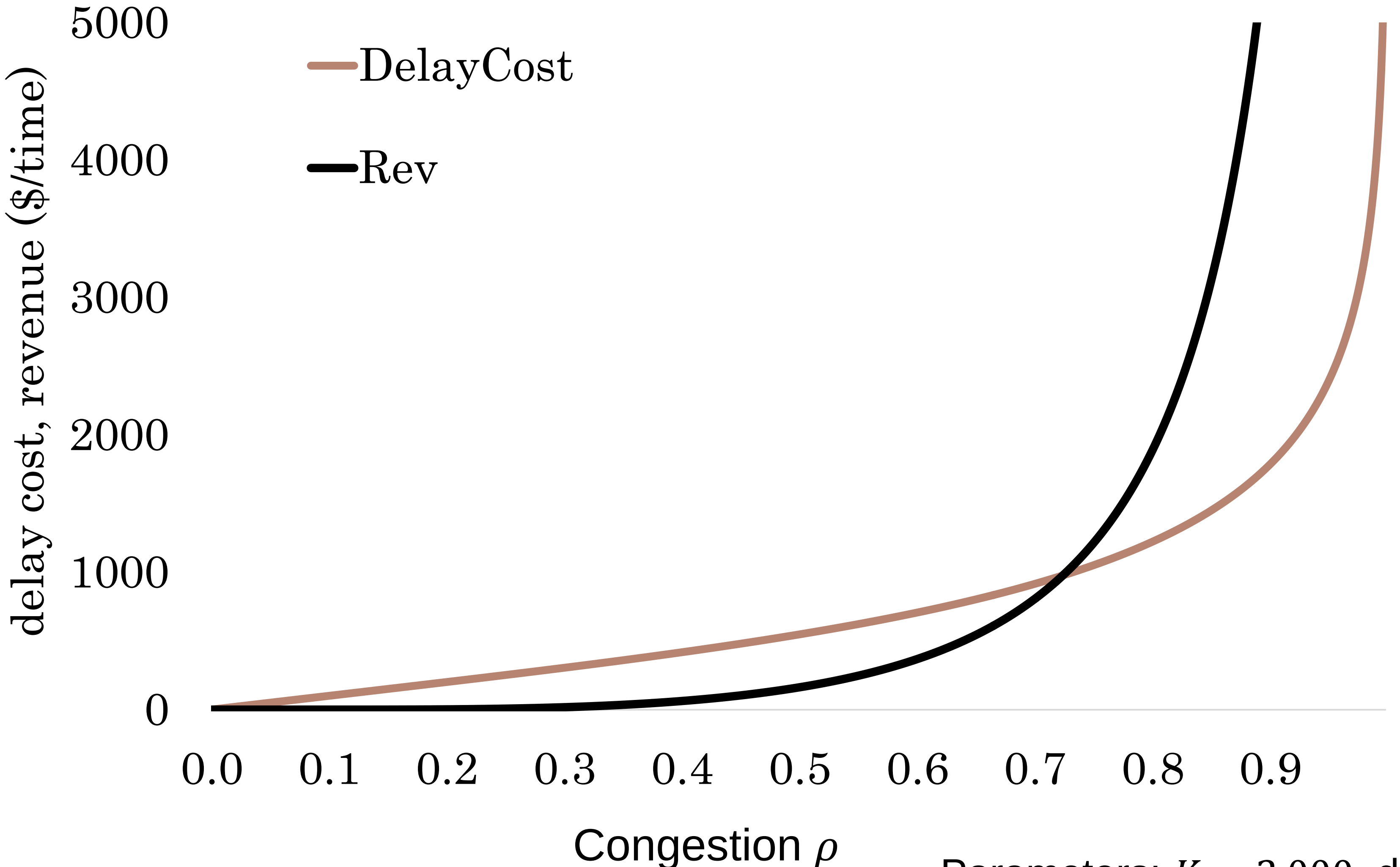
$$DelayCosts = K\rho \int_0^{\bar{c}} cf\left(c\right) \cdot W_K\left(\rho\bar{F}\left(c\right)\right) dc$$

$$Rev = K\rho^2 \int_0^{\bar{c}} cf\left(c\right) \bar{F}\left(c\right) \cdot W_K'\left(\rho\bar{F}\left(c\right)\right) dc$$

and

$$N = Rev/c_m.$$

Equilibrium Revenue and Delay Costs



Parameters: $K = 2{,}000$, delay costs distributed $c \sim U[0,1]$

Equilibrium Fees and Delays

Corollary:

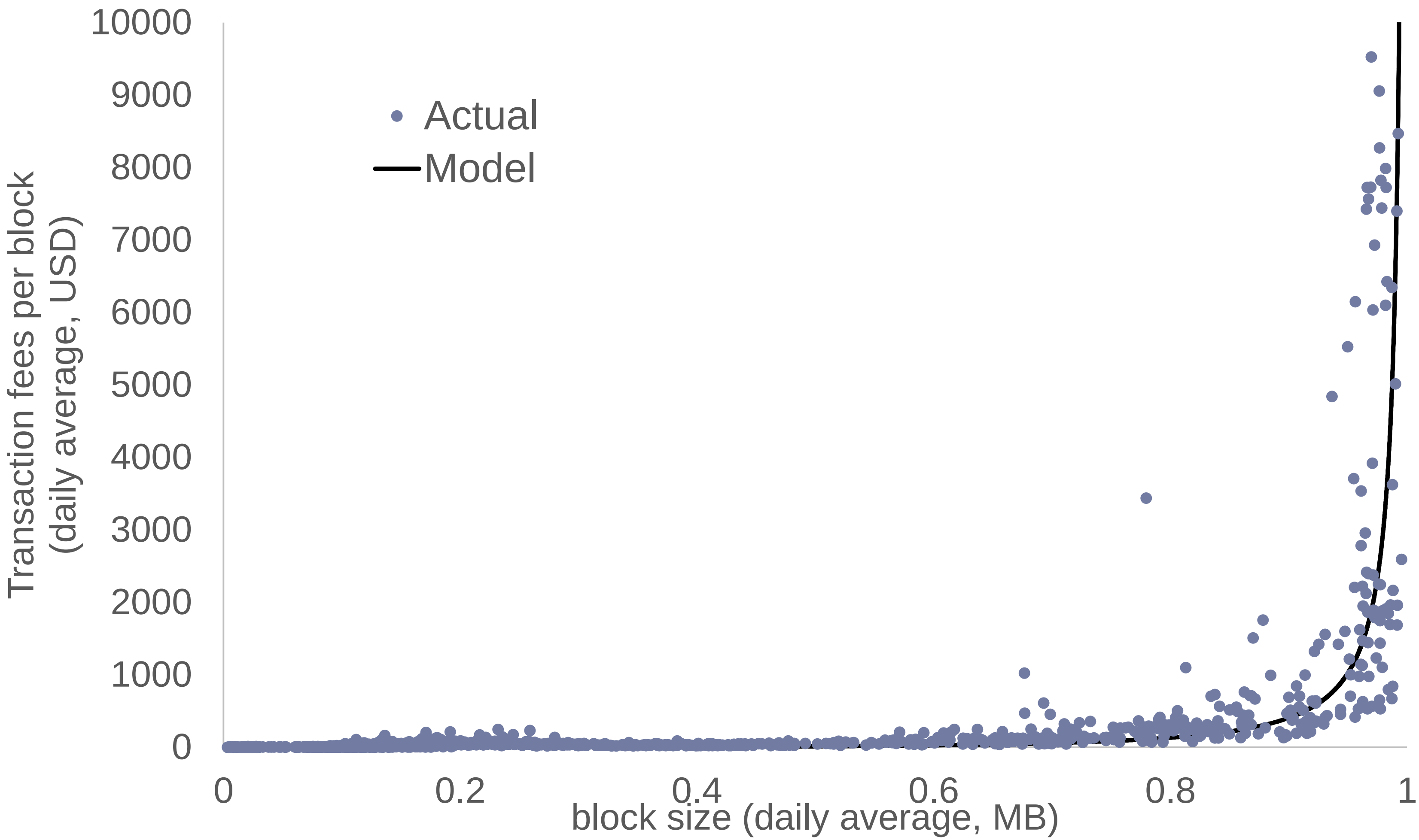
Equilibrium revenue (total fees), infrastructure level, and delay costs are increasing with congestion

$$Rev'(\rho) = K\rho \int_0^\infty \bar{W}'\left(\rho \bar{F}(c)\right) \bar{F}(c)^2 \, dc > 0$$

$$DC'(\rho) = (DC(\rho) + Rev(\rho))/\rho > 0$$

When $\rho = 0$ both Rev and DC are zero.

Data: Total Transaction Fees vs Congestion



Model curve parameters: $K = 2{,}000$, and delay costs $c \sim U[0{,}0.1]$ for 10min.

Revenue and infrastructure

- Infrastructure provided at cost
  - Free entry/exit, competition of miners
- Revenue and infrastructure vary with congestion
  - Revenue determines infrastructure level, but revenue does not depend on the need for infrastructure
  - Infrastructure level can be too low or too high
- Congestion and delay costs are necessary for positive revenue

Potential Instability

Corollary: *No Delays ⇒ No Revenues*

- Low utilization ρ implies low revenue, miners exit
- Miners' exit does not generate congestion
  - System throughput is independent of number of miners
- System becomes unreliable with low number of miners (latency, vulnerability)
  - Potentially reducing user demand and ρ
  - Bad dynamics, leads to system collapse

Summary: Costs, Potential Waste

- Costly design
  - Redundancies, Tournament for random selection
- Delay costs are necessary to incentivize payment
- Infrastructure level (number of miners) may not be optimal
  - Determined by transaction fee payments due to congestion, not the need for more miners

- Costs can be smaller or larger than monopoly deadweight loss

Design: Controlling μ and K

- Instead of having a fixed capacity, we consider adjusting μ and K according to realized demand
  - Can be implemented in equilibrium, abstracting away from technological limits (such as network latency)
  - Need to understand the effect of bigger blocks versus more frequent blocks

Approximation for large K

Theorem:

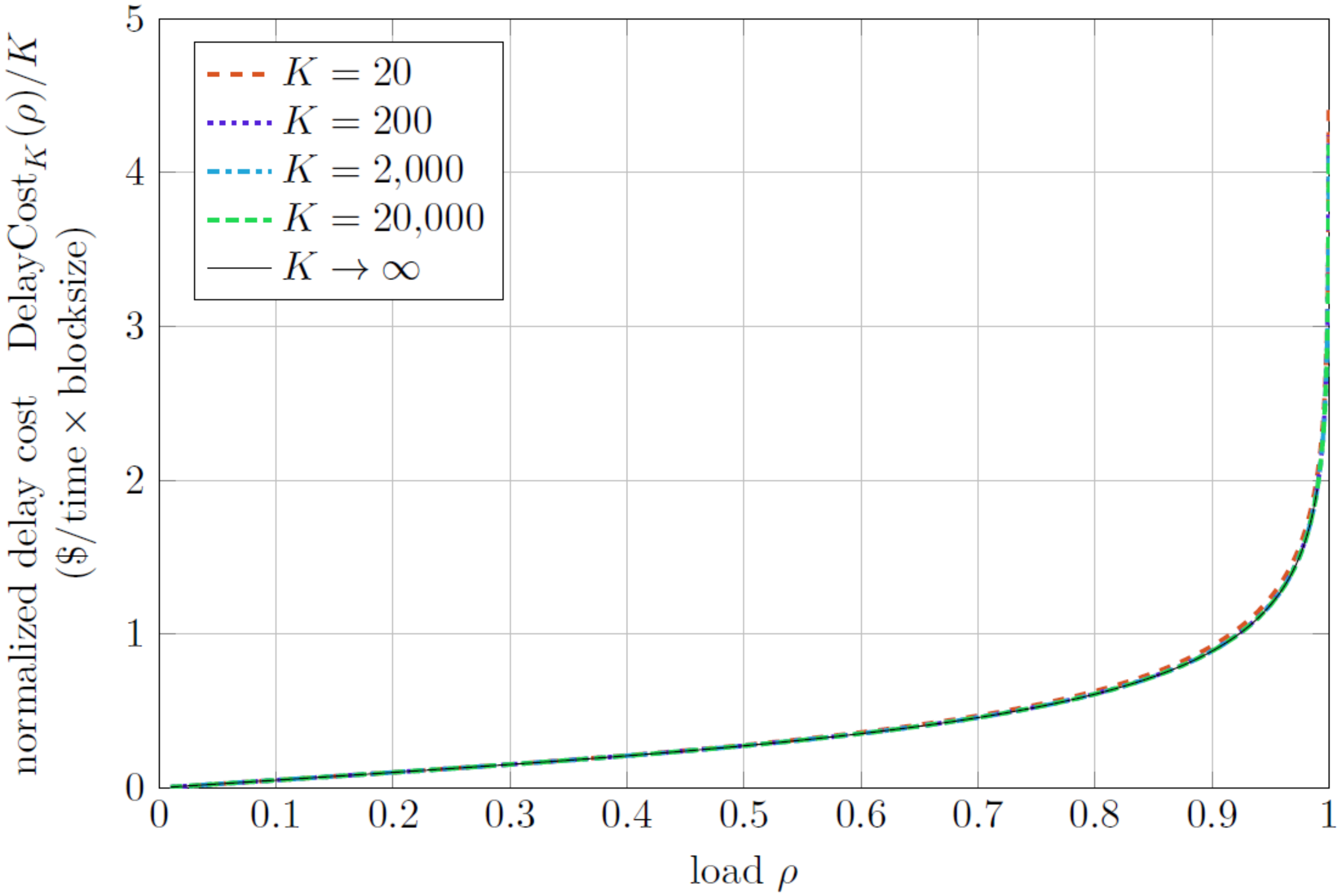
As the block size K increases we have that

$$\lim_{K\to\infty} W_K(\hat{\rho}) = W_\infty(\hat{\rho})$$

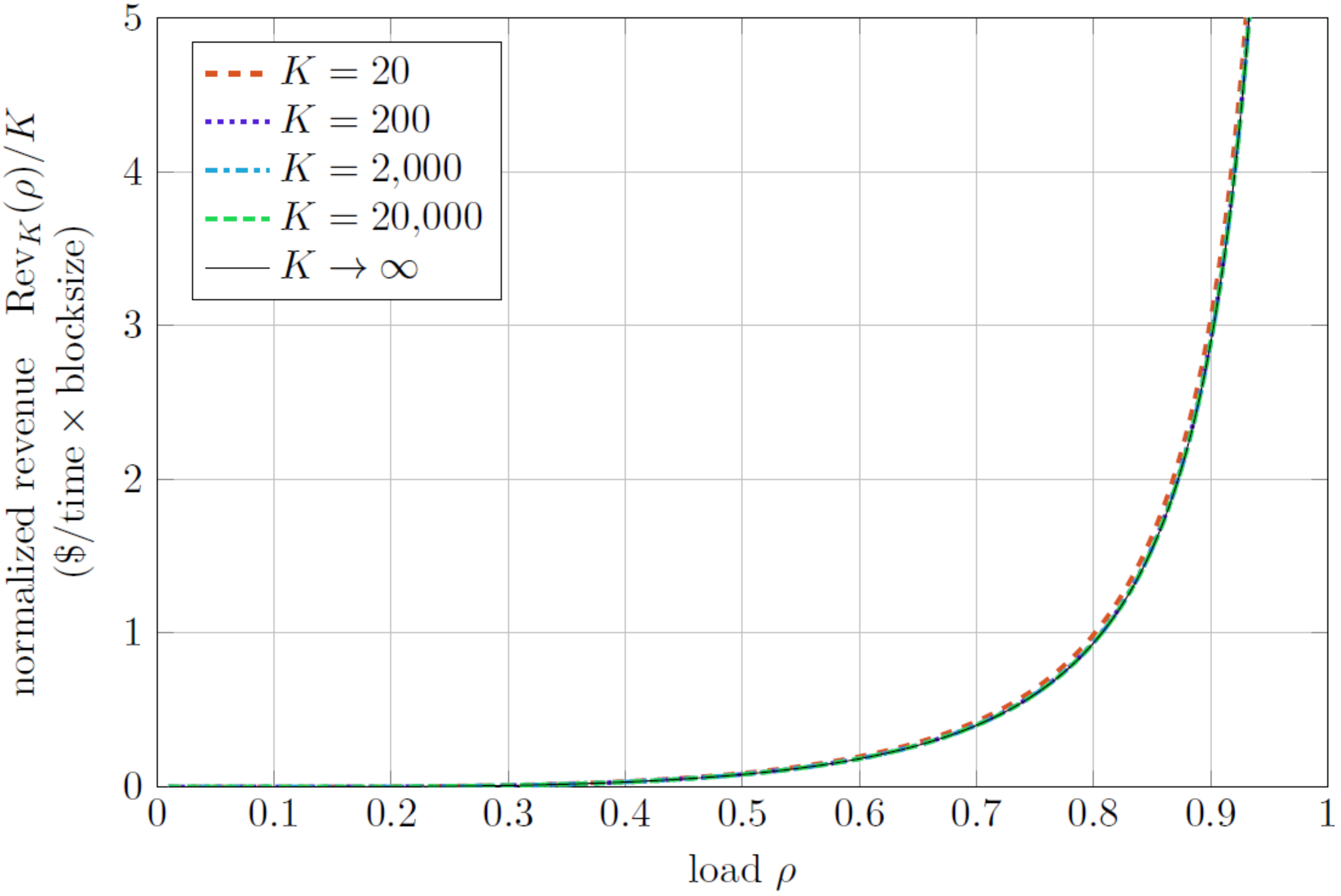
and

$$\mathrm{Rev}_K(\rho) = K \cdot \mathrm{Rev}_\infty(\rho) + o(K),$$
$$\mathrm{DelayCost}_K(\rho) = K \cdot \mathrm{DelayCost}_\infty(\rho) + o(K).$$

Convergence for Large K



Convergence for Large K



Revenue and Delay for Neglible Congestion

Theorem:

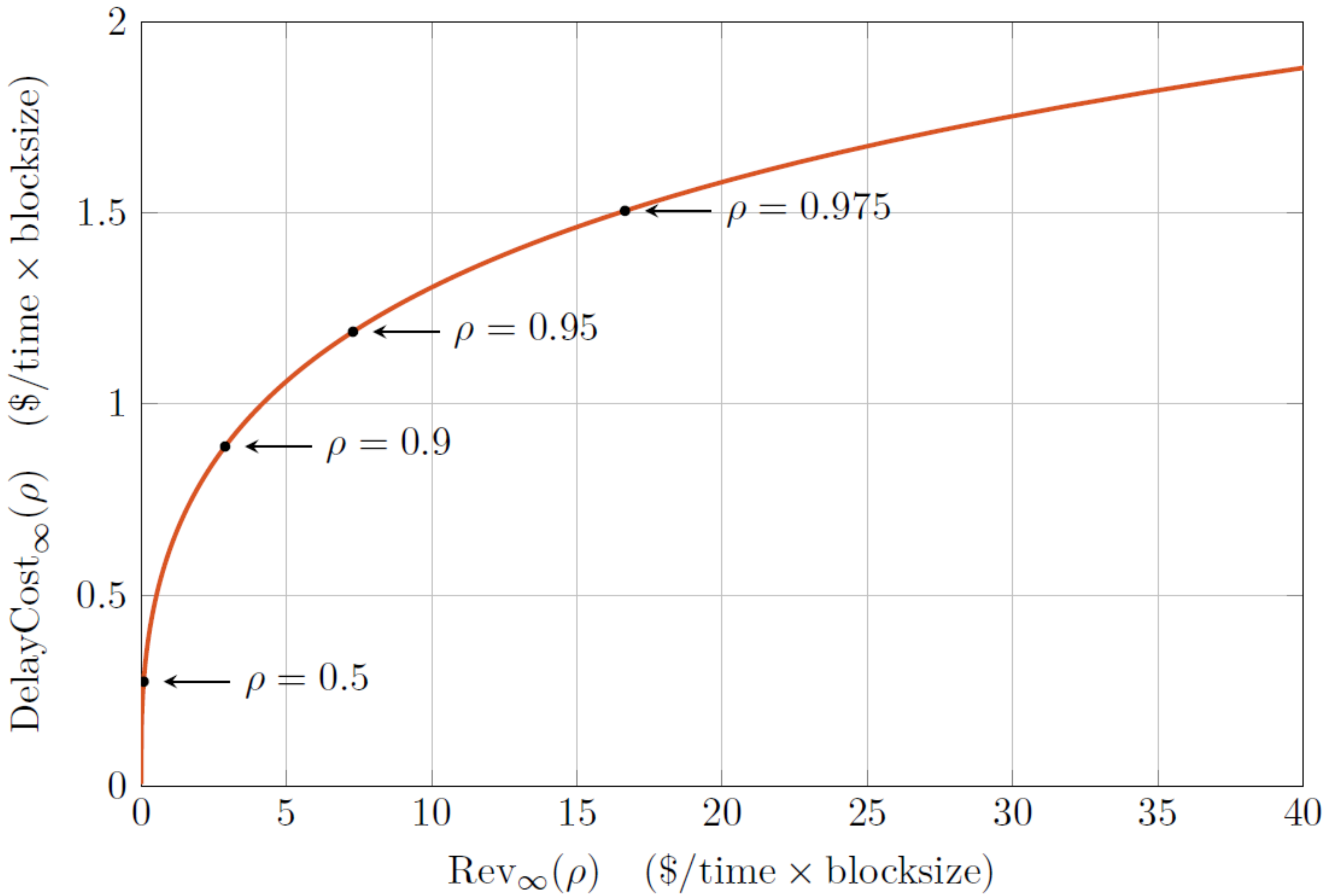
As $\rho \to 0$ we have that

$$\mathrm{Rev}_{\infty}(\rho) = O\left(e^{-1/\rho}\right),$$

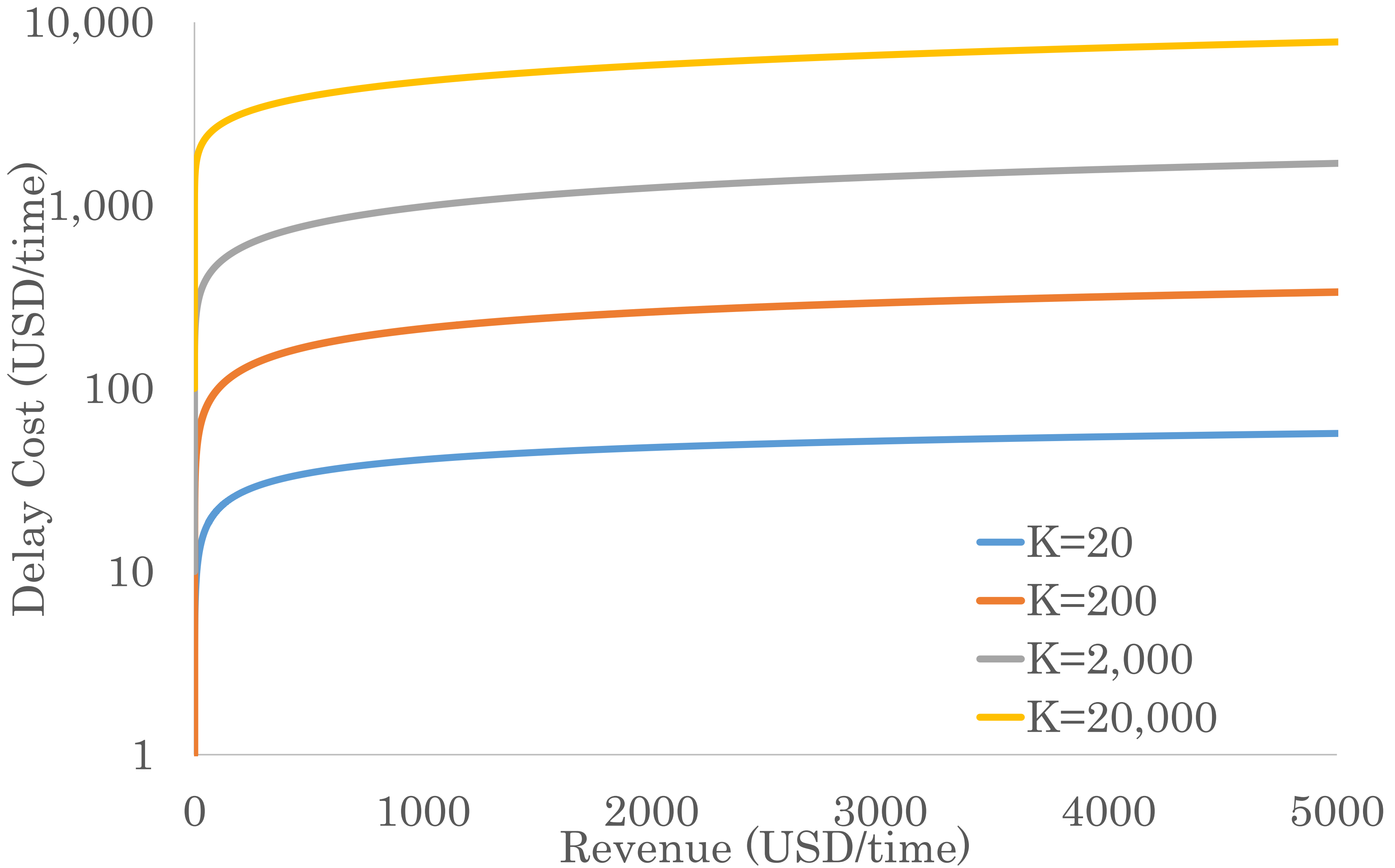
$$\mathrm{DelayCost}_{\infty}(\rho) = \rho \cdot E\left[c\right] + o\left(\rho\right).$$

That is, delay costs are much larger than revenue for small ρ.

Controlling Congestion



Controlling Congestion



Summary

- Economic innovation of Blockchain technology
  - No owner
  - Competitive pricing, even if the platform is a monopoly
  - Fees determined in equilibrium

- Congestion as a revenue generating mechanism
  - System can raise revenue while serving all potential users
  - Requires congestion, delay costs

- Design of revenue generating rules
  - Control congestion to target revenue
  - Benefit of smaller block size
  - Future work – what revenue generating rules are implementable?