The Economics of the Bitcoin Payment System

Jacob Leshno, Chicago Booth
Based on work with Ciamac Moallemi and Gur Huberman, Columbia Business School

ECONOMETRICA
JOURNAL OF THE ECONOMETRIC SOCIETY

The Economist as Engineer: Game Theory, Experimentation, and Computation as Tools for Design Economics†

Alvin E. Roth

First published: 12 December 2003 | https://doi.org/10.1111/1468-0262.00335 |

Abstract

Economists have lately been called upon not only to analyze markets, but to design them. Market design involves a responsibility for detail, a need to deal with all of a market's complications, not just its principle features. Designers therefore cannot work only with the simple conceptual models used for theoretical insights into the general working of markets. Instead, market design calls for an engineering approach. Drawing primarily on the design of the entry level labor market for American doctors (the National Resident Matching Program), and of the auctions of radio spectrum conducted by the Federal Communications Commission, this paper makes the case that experimental and

Who Gets What — and Why

ALVIN E. ROTH

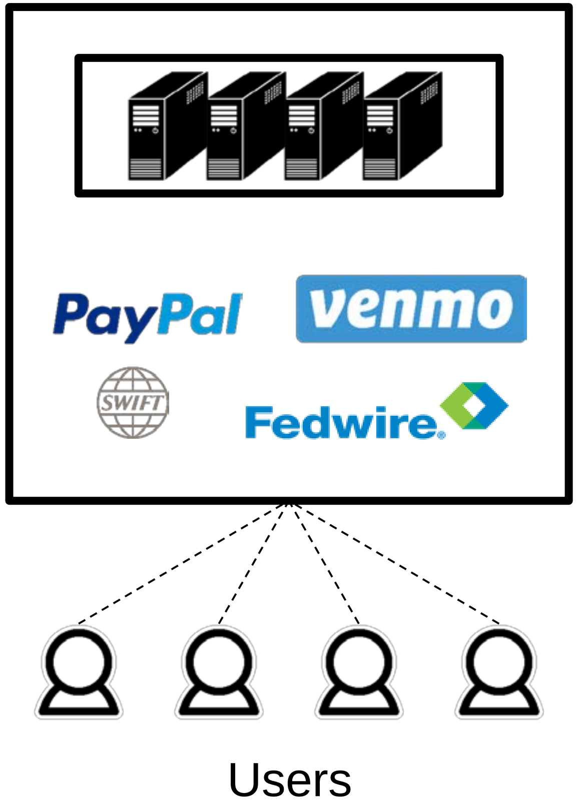
Winner of
THE NOBEL PRIZE IN ECONOMICS

Top 100 Cryptocurrencies by Market Capitalization

Cryptocurrencies ▾ | Exchanges ▾ | Watchlist | USD ▾ | Next 100 → | View All

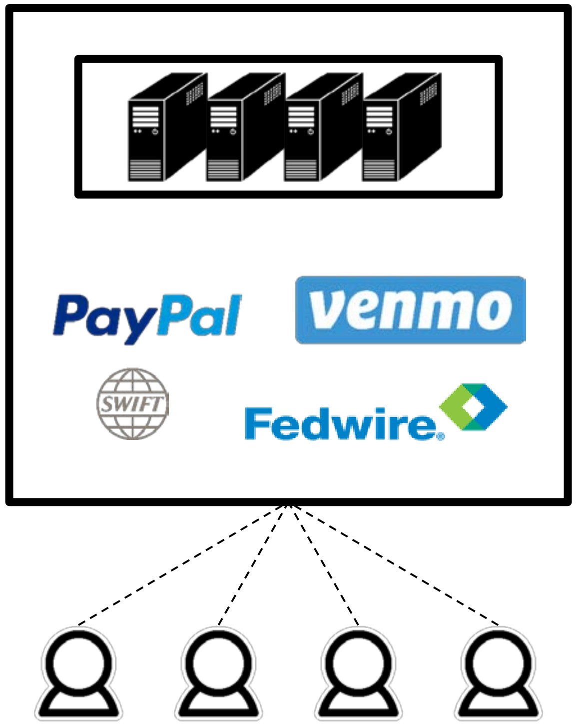
#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)	
1	Bitcoin	$203,918,783,289	$11,410.73	$15,705,918,263	17,870,787 BTC	0.09%		···
2	Ethereum	$22,919,531,662	$213.64	$6,292,005,275	107,278,818 ETH	3.88%		···
3	XRP	$13,040,650,220	$0.304172	$849,774,753	42,872,646,068 XRP *	2.31%		···
4	Bitcoin Cash	$5,960,916,360	$332.24	$1,170,302,065	17,941,688 BCH	6.78%		···
5	Litecoin	$5,675,202,358	$90.06	$3,121,584,226	63,014,981 LTC	5.67%		···
6	Binance Coin	$4,654,460,896	$29.93	$266,480,436	155,536,713 BNB *	1.44%		···
7	Tether	$4,048,830,914	$1.00	$16,109,366,785	4,043,425,265 USDT *	0.21%		···
8	EOS	$3,869,415,583	$4.17	$1,588,287,781	927,033,053 EOS *	3.99%		···
9	Bitcoin SV	$2,594,547,869	$145.31	$303,608,935	17,854,986 BSV	3.09%		···
10	Monero	$1,571,885,968	$91.66	$76,016,856	17,148,987 XMR	0.26%		···
11	Stellar	$1,547,268,940	$0.078812	$77,262,899	19,632,397,508 XLM *	8.09%		···

Traditional Payment Systems



- Require trust

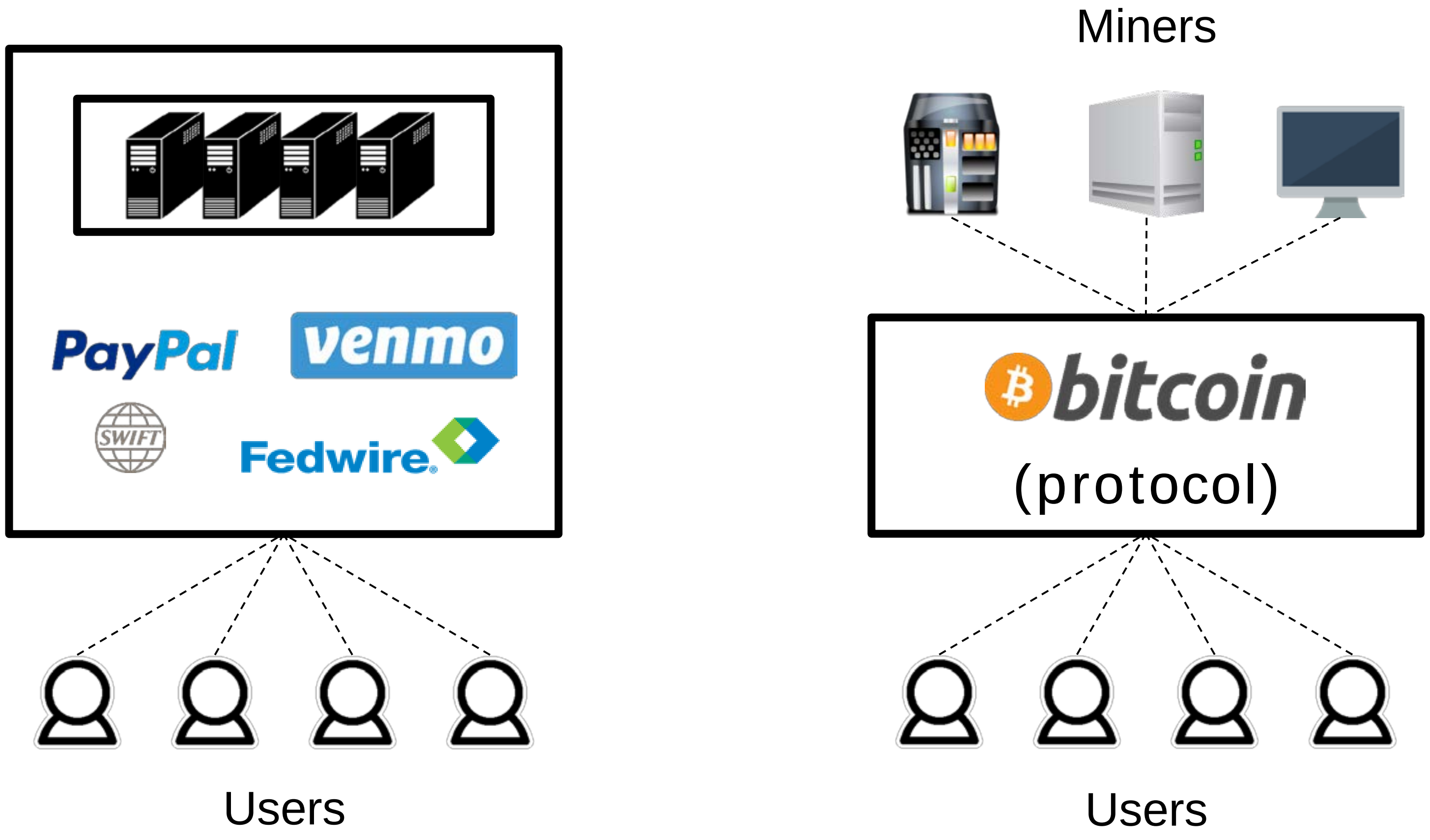
Traditional Payment Systems



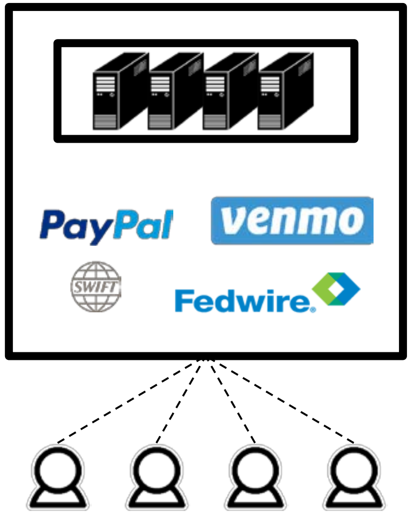
Users

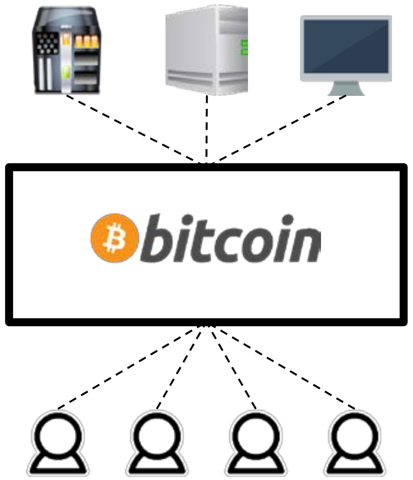
- ~~Require trust~~
- Monopoly deadweight loss
  - Price too high, potential users excluded
- Hold-up
  - Price will increase if users are lock in
  - Prevents ex-ante adoption

Traditional Payment Systems vs. Bitcoin



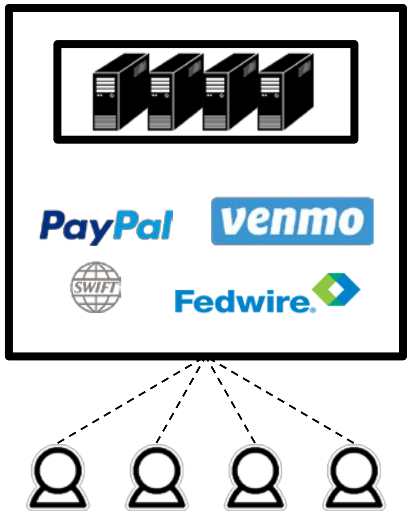
Traditional Payment Systems vs. Bitcoin

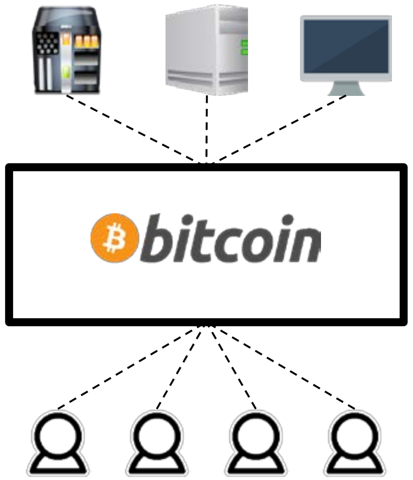




Rules	Set by firm/org	Fixed by protocol
Infrastructure	Procured by firm/org	
Pricing	Fees set by firm/org	
Balancing supply and demand	Firm's incentives	

Traditional Payment Systems vs. Bitcoin





Rules	Set by firm/org	Fixed by protocol
Infrastructure	Procured by firm/org	*Entry/Exit, Revenue*
Pricing	Fees set by firm/org	*Equilibrium congestion pricing, Miners do not set prices*
Balancing supply and demand	Firm's incentives	*??*

Bitcoin as a Two-Sided Market – key properties

- Users choose transaction fees

- Miners choose pending transactions to include in their block
- System's capacity is independent of number of miners
  - One miner selected at random to process transactions
  - Block size and block rate fixed by protocol
- New blocks are added as a Poisson process
- Free entry and exit of miners
  - Approximate (ignoring ASICs etc)
  - Assume there are many small miners with a cost c_m

Simplified Economic Model

- N computing units of miners
  - Many potential small miners whose cost is c_m
  - Free entry/exit
- Blocks added at rate μ, each can process K transactions
  - System's capacity is $K \cdot \mu$
- Users/transactions
  - Receive utility from service $R - c \cdot W - b$
  - Heterogeneous delay cost c
  - Willingness to pay R_H or R_L, equal prob (ind of c)
  - Arrive at Poisson rate $\lambda < K \cdot \mu$ (excess capacity)

Benchmark: Dead-weight Loss Under a Profit Maximizing Firm

A profit maximizing firm sets a high transaction fee excluding low WTP customers, processes transactions without delay.

- Monopoly dead-weight loss
  - Not serving low willingness to pay users, although it can efficiently do so
- Prices go up if users are locked in and their WTP increases

Bitcoin Miners: No Pricing Power

Suppose that some small miners are active.
Then no miner can profitably affect transaction fees, including large miners.

- All miners select highest paying transactions
- That is, in equilibrium miners are price takers
- Large miners can affect transaction fees, but that will spur entry and won't raise their revenue

Bitcoin Miners: Number of Miners

- Total payment to miners is equal to total transaction fees Rev plus the value of minted coins $s \cdot e$ (both in USD)
- Expected payment per mining unit is $(Rev + s \cdot e)/N$
- Free entry of small miners with cost c_m implies small miners break even

The equilibrium number of miners is

$$N = \frac{Rev + s \cdot e}{c_m}$$

Data: Miners Costs and Revenue Oct 2015

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

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

- Approx. $325M annually

Approx. total reward:

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

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

Bitcoin Users: Choice of Transaction Fees

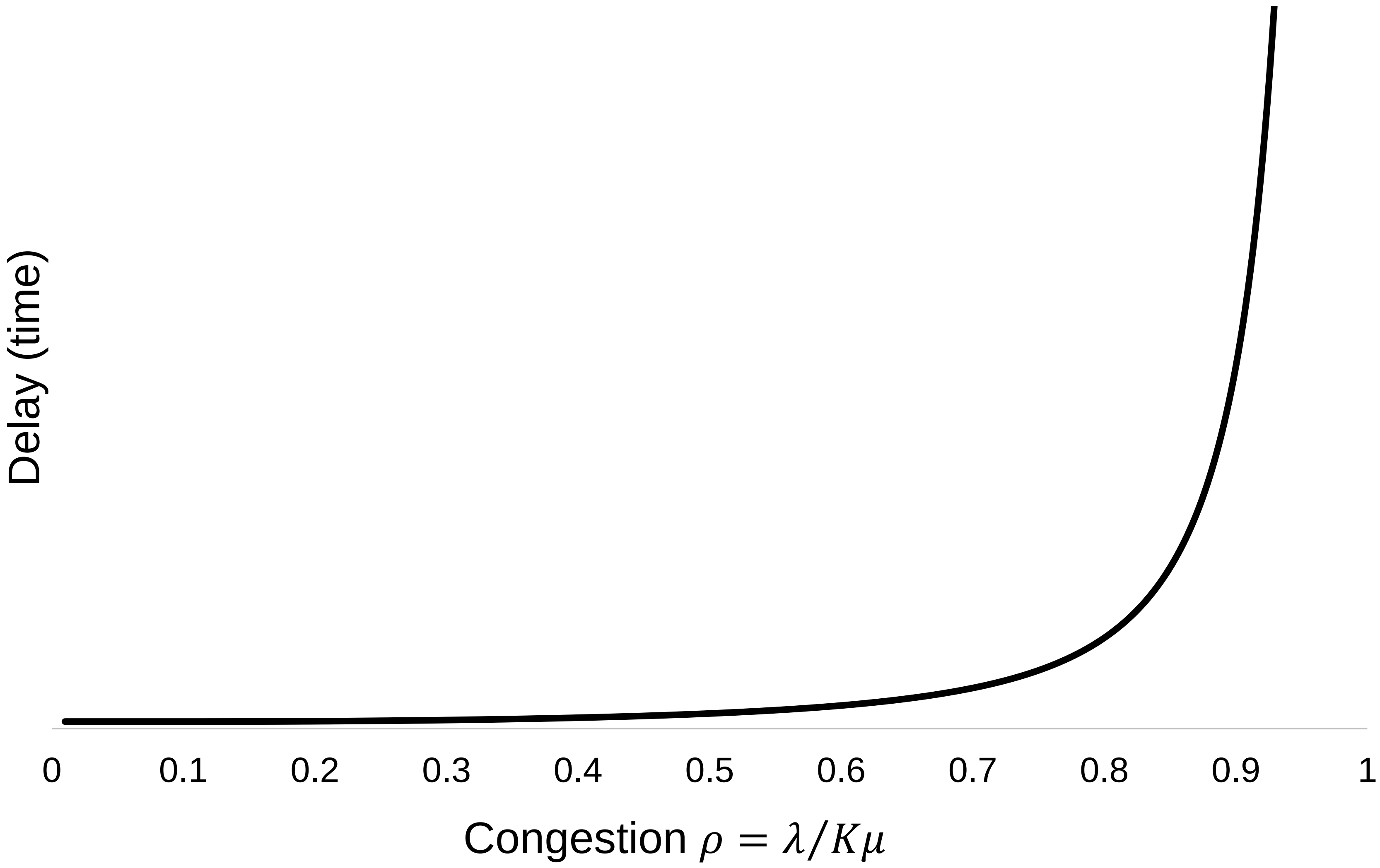
- Users choose transaction fees b_i to maximize

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

  where $W(b_i|G)$ is expected delay given distribution of others' bids G

- Users play a congestion queueing game
  - Participate or not
  - Trade off transaction fees b_i and delay $W(b_i|G)$
  - Independent of number of miners

Expected Delay for Lowest Priority Transaction given Congestion ρ

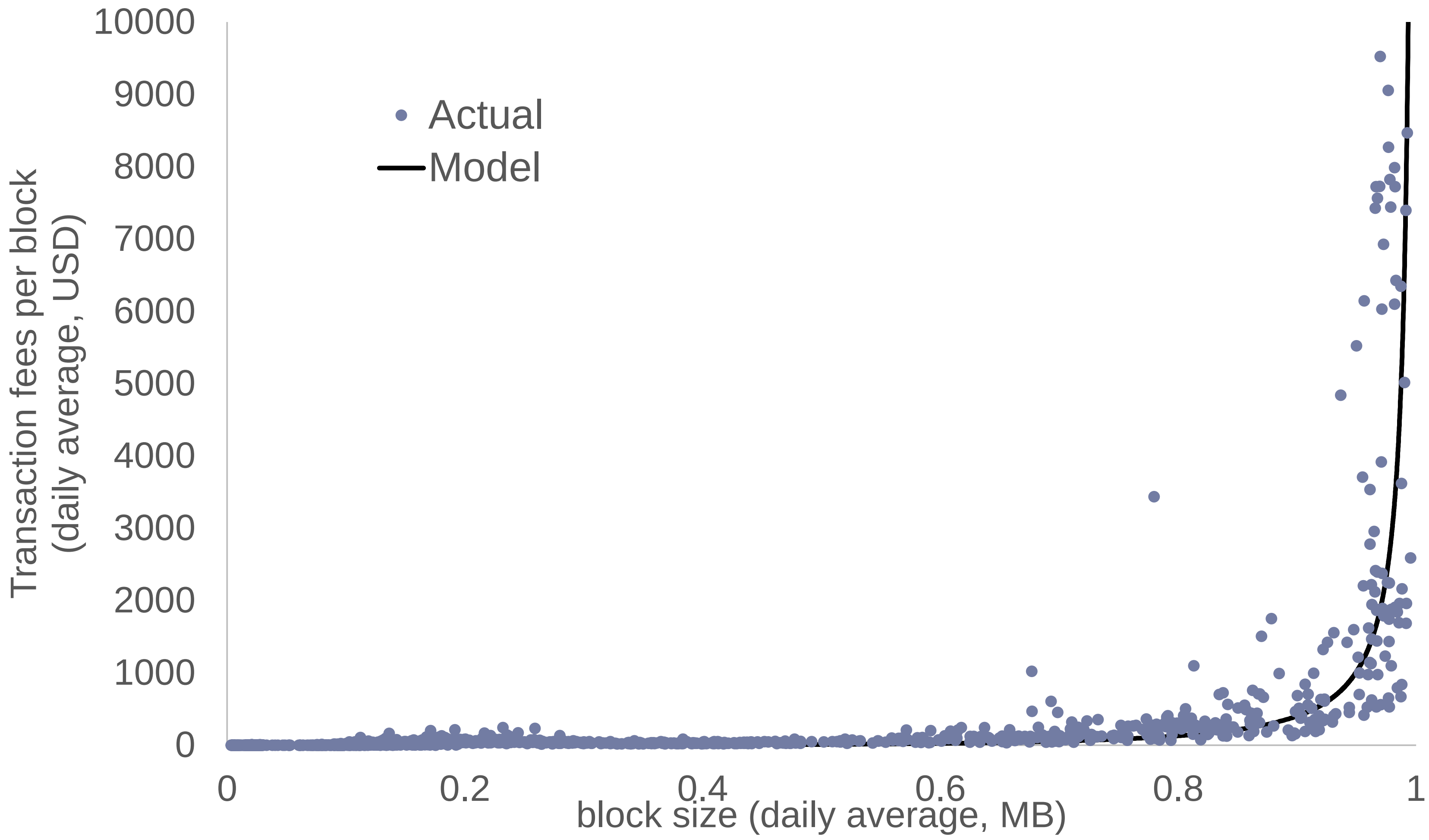


Analysis of Users/Transactions

Assuming WTP sufficiently high and the system has excess capacity, in equilibrium:

- All users participate
- Impatient users costs pay higher transaction fees, receive higher priority and lower delay
- Transaction fees equal to the delay externality imposed on other transactions
- Transaction fees independent of WTP, but depend on congestion

Data: Total Transaction Fees vs Congestion



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

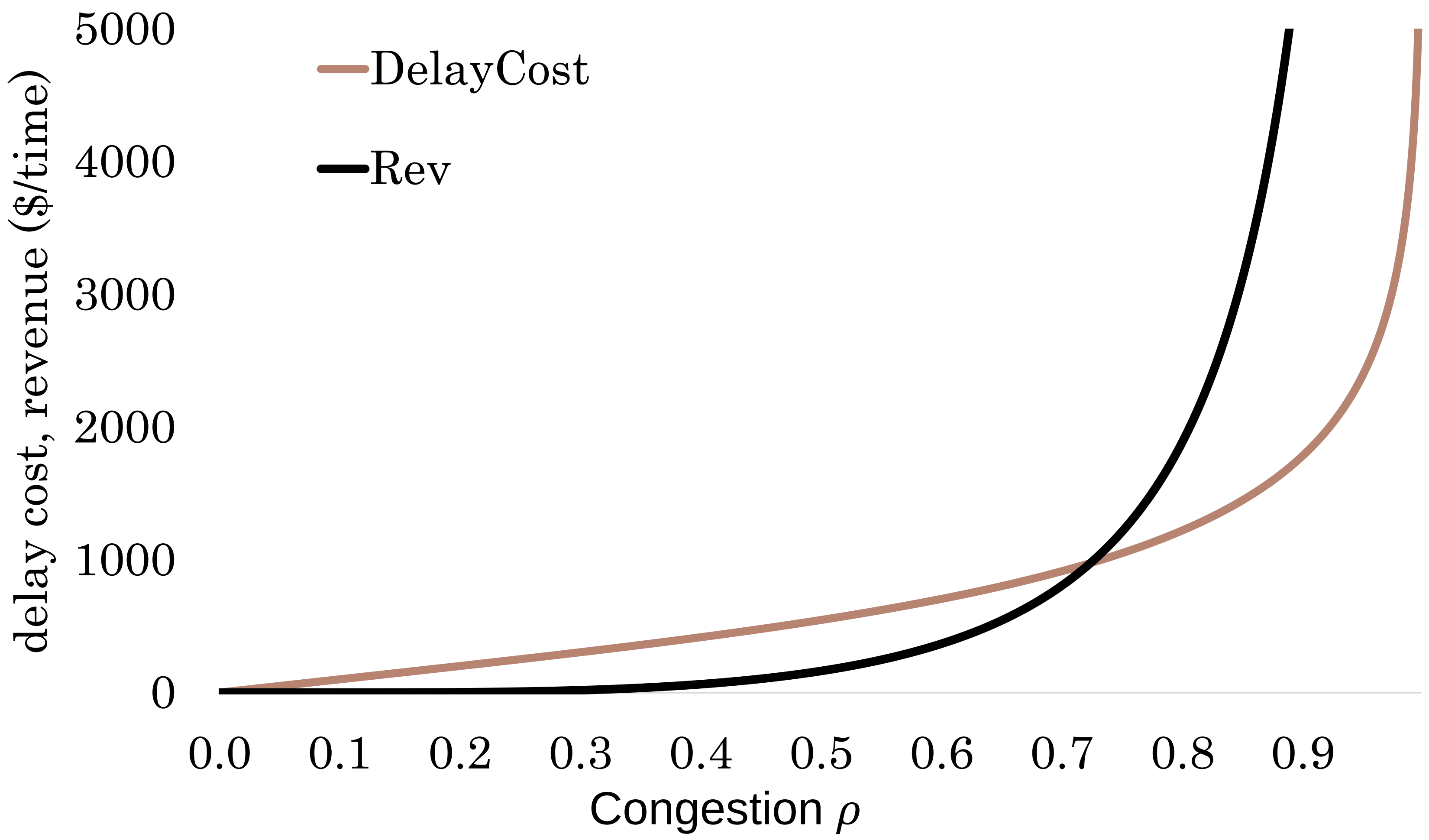
Transaction Fees

- Positive revenue, without excluding transactions
  - Even transaction that pay no fee are processed
- Strictly positive net reward to all users
  - Not possible under a profit maximizing firm
- Payments do not depend on willingness to pay, if it is sufficiently enough
  - No monopoly pricing, even if the system is a monopoly
  - No hold-up

But:

- Fees vary with congestion ρ
- Fees independent of need for infrastructure

Revenue and Delay Costs Given ρ



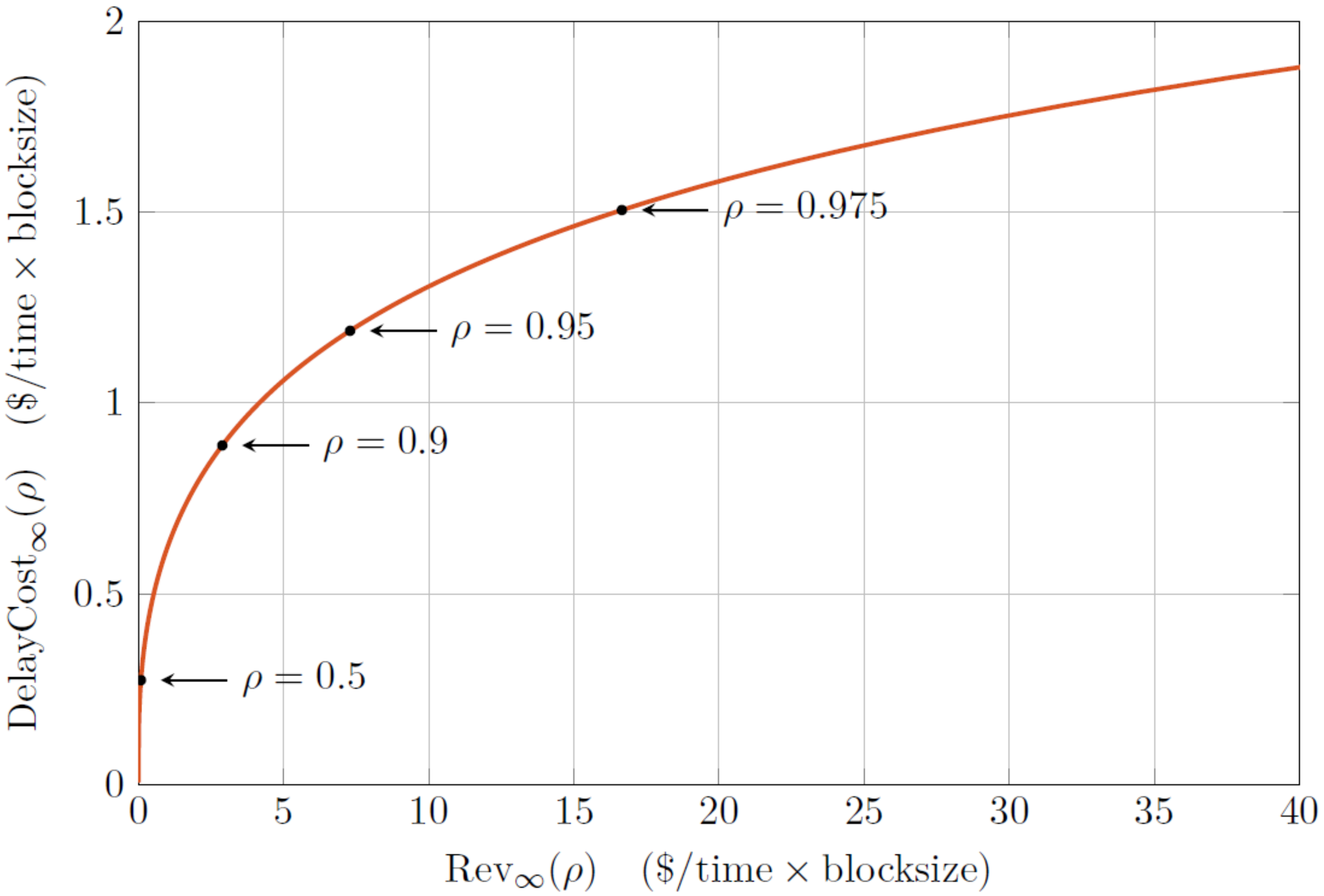
Parameters: $K = 2{,}000$, delay costs distributed $c \sim U[0,1]$

Welfare Under Bitcoin

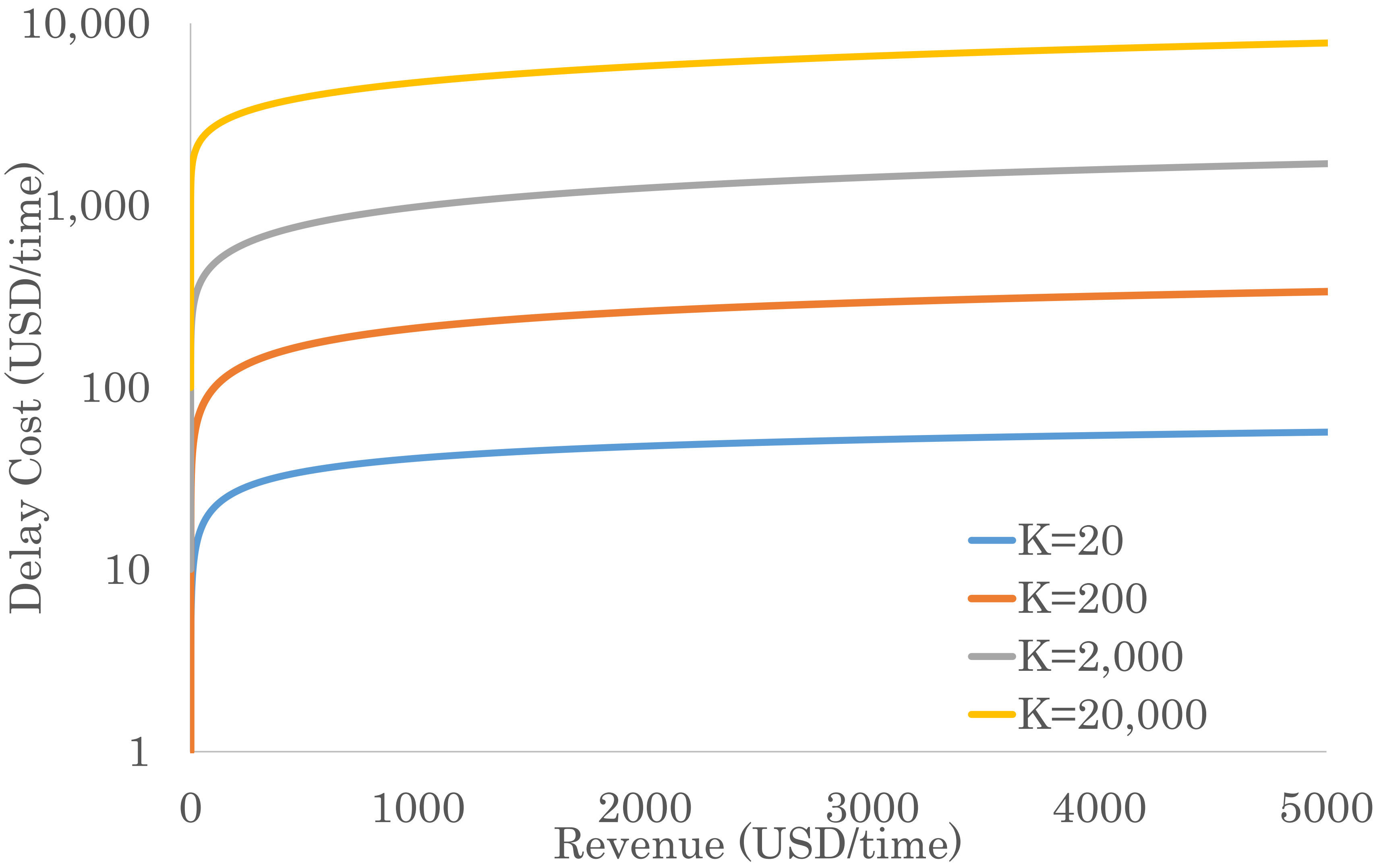
- Costly design
  - Redundancies, Tournament for random selection
- Delay costs are necessary to incentivize payment
- Infrastructure level likely to be suboptimal
  - Transaction fees vary with congestion
  - Block reward varies with exchange rate (currently the majority of the reward)

Welfare can be larger under Bitcoin if these are less than monopoly deadweight loss

Controlling Congestion – Revenue vs. Delay



The Tradeoff Between Congestion and Delay for Different Maximal Block Size



Summary

- Economic innovation of Blockchain is governance
  - No owner, commitment to rules
  - Fees determined in equilibrium, miners are price takers
- Congestion as a revenue generating mechanism
  - Can raise revenue without excluding users
  - Requires delay costs, inefficient at raising low amounts
  - Importance of stochastic block-arrival process
- Market fails to balance supply and demand
  - Can control congestion to target revenue
  - Benefit of smaller block size

Blockchain

- Blockchain blockchain blockchain blockchain, blockchain Bitcoin blockchain blockchain
- Blockchain blockchain blockchain blockchain
  - Blockchain blockchain blockchain blockchain blockchain, blockchain blockchain blockchain blockchain.
  - Machine learning blockchain blockchain blockchain
- Decenterlized blockchain blockchain blockchain
- Blockchain blockchain blockchain!