Monopoly Without Monopolist: Economics of the Bitcoin Payment System

Jacob Leshno, Chicago Booth
joint work w. Gur Huberman, Ciamac Moallemi
Cryptocurrencies

- Decentralized Electronic payment systems
  - Bitcoin being the first, many other followed and offer different functions

- Decentralized, two-sided markets
  - Users receive similar services to PayPal, Fedwire
  - Miners provide infrastructure
  - Security and Market design enabled by blockchain protocol

- Novel economic structure
  - Owned by no one
  - Rules fixed by a computer protocol
  - Participants are price-takers
Cryptocurrencies

CryptoCurrency Market Capitalizations

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


Huberman, Leshno, Moallemi – Economic Analysis of Bitcoin
Traditional Payment Systems
Traditional Payment Systems

- Monopoly deadweight loss (price too high)
- Hold-up

Huberman, Leshno, Moallemi – Economic Analysis of Bitcoin
Traditional Payment Systems vs. Bitcoin

Huberman, Leshno, Moallemi – Economic Analysis of Bitcoin
# Traditional Payment Systems vs. Bitcoin

<table>
<thead>
<tr>
<th></th>
<th>Traditional Systems</th>
<th>Bitcoin</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rules</strong></td>
<td>Set by firm/org</td>
<td>Fixed by protocol</td>
</tr>
<tr>
<td><strong>Infrastructure</strong></td>
<td>Procured by firm/org</td>
<td></td>
</tr>
<tr>
<td><strong>Pricing</strong></td>
<td>Fees set by firm/org</td>
<td></td>
</tr>
<tr>
<td><strong>Balancing supply and demand</strong></td>
<td>Firm’s incentives</td>
<td></td>
</tr>
</tbody>
</table>

Huberman, Leshno, Moallemi – Economic Analysis of Bitcoin
# Traditional Payment Systems vs. Bitcoin

<table>
<thead>
<tr>
<th></th>
<th>Traditional Payment Systems</th>
<th>Bitcoin</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rules</strong></td>
<td>Set by firm/org</td>
<td>Fixed by protocol</td>
</tr>
<tr>
<td><strong>Infrastructure</strong></td>
<td>Procured by firm/org</td>
<td>Entry/Exit, Revenue</td>
</tr>
<tr>
<td><strong>Pricing</strong></td>
<td>Fees set by firm/org</td>
<td>Equilibrium congestion pricing</td>
</tr>
<tr>
<td><strong>Balancing supply and demand</strong></td>
<td>Firm’s incentives</td>
<td>??</td>
</tr>
</tbody>
</table>

Huberman, Leshno, Moallemi – Economic Analysis of Bitcoin
The Blockchain ledger

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

Huberman, Leshno, Moallemi – Economic Analysis of Bitcoin
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

Huberman, Leshno, Moallemi – Economic Analysis of Bitcoin
Blockchain

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

Huberman, Leshno, Moallemi – Economic Analysis of Bitcoin
Blockchain

- New transactions transmitted to all miners

Huberman, Leshno, Moallemi – Economic Analysis of Bitcoin
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

Huberman, Leshno, Moallemi – Economic Analysis of Bitcoin
Blockchain

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

Huberman, Leshno, Moallemi – Economic Analysis of Bitcoin
Blockchain

Huberman, Leshno, Moallemi – Economic Analysis of Bitcoin
Bitcoin as a Two-Sided Market

- Users choose transaction fees
- Miners choose pending transactions to include in their block
- New blocks are added as a Poisson process
- System’s throughput is independent of number of miners
  - One miner selected at random to process transactions
  - Block size and block rate fixed by protocol
- Free entry and exit of miners

Huberman, Leshno, Moallemi – Economic Analysis of Bitcoin
Simplified Economic Model

- \( N \) computing units of miners
  - Many potential small miners whose cost is \( c_m \)
  - Free entry/exit
- Blocks added at rate \( \mu \), 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)
A Profit Maximizing Firm: 
Dead-weight Loss

Suppose $1/2 R_H > R_L$. A profit maximizing firm sets a transaction fee equal to $R_H$, processes transactions without delay.

- Monopoly dead-weight loss is $1/2 R_L$
  - Not serving low willingness to pay users
- 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 $(Rev + s \cdot e)/N$
- Small miners need to 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):

\[ 1.6 \text{tx/sec} \cdot \$6/\text{tx} \approx \$10/\text{sec} = \$6,000/10\text{min} \]

- Approx. $325M annually

Approx. total reward:

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

- [http://www.coinwarz.com/cryptocurrency](http://www.coinwarz.com/cryptocurrency)

Huberman, Leshno, Moallemi – Economic Analysis of Bitcoin
Bitcoin Users: Choice of Transaction Fees

- Users choose transaction fees $b_i$ to maximize

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

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 $W(b_i|G)$
  - Independently of number of miners

Huberman, Leshno, Moallemi – Economic Analysis of Bitcoin
Analysis of Users/Transactions

- Solving for the stochastic behavior of the system

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

\( \rho = \lambda/\mu K \) is congestion/load

\( \rho \bar{F}(c_i) \) is effective congestion for \( c_i \)
Expected Wait Formulas

Using generating functions, the expected wait of a transaction is

\[ \mu^{-1} W_K (\hat{\rho}) = \frac{1}{\mu (1 - z_0)} \frac{1}{1 + K \hat{\rho} + (K + 1) z_0^K} \]

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

\[ z_0^{K+1} - (K \hat{\rho} + 1) z_0 + K \hat{\rho} = 0 \]
Expected Delay for Lowest Priority Transaction given Congestion $\rho$

Congestion $\rho = \lambda / K\mu$

Huberman, Leshno, Moallemi – Economic Analysis of Bitcoin
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.

\[
b(c_i) = \rho \int_0^{c_i} f(c) \cdot c \cdot \mu^{-1} W'_K (\rho \bar{F}(c)) \, dc
\]

\[
u(c_i) = R - \int_0^{c_i} \mu^{-1} W_K (\rho \bar{F}(c)) \, dc
\]
Assuming WTP sufficiently high, 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, depend on congestion $\rho = \lambda/\mu K$
Model curve parameters: $K = 2,000$, and delay costs $c \sim U[0,0.1]$ for 10 min.

Huberman, Leshno, Moallemi – Economic Analysis of Bitcoin
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 $\rho$
- Fees independent of need for infrastructure
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 $K$.

\[
\text{DelayCosts} = K\rho \int_0^{\bar{c}} c f(c) \cdot W_K \left(\rho \bar{F}(c)\right) dc
\]

\[
Rev = K\rho^2 \int_0^{\bar{c}} c f(c) \bar{F}(c) \cdot W'_K \left(\rho \bar{F}(c)\right) dc
\]

and

\[
N = Rev/c_m.
\]
Revenue and Delay Costs Given $\rho$

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
Modifying the Design

- Current protocol fixes block-rate $\mu$, block-size $K$,
  - Congestion and revenue vary with demand $\lambda$
  - Revenue may be too high or too low

- What about a fixed transaction fee?
  - Denominated in coin
  - Fluctuates with exchange rate, can be too high or too low
  - Same holds for mining rewards

- Can we use the market?
Design Modification: Stable Congestion

- Target stable congestion $\rho$
  - set $\mu$ and $K$ according to demand
  - Congestion below 100% is observable on chain
  - Can adjust hash-difficulty, block size according to on-chain congestion (within limits)

- Achieves stable revenue in USD
  - Using the “market for delays”

- How to set parameters $\mu$, $K$?
  - Bigger blocks or more frequent blocks?
  - Tradeoff between Delay Costs and Revenue

Huberman, Leshno, Moallemi – Economic Analysis of Bitcoin
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

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

$$\text{DelayCost}_K(\rho) = K \cdot \text{DelayCost}_\infty(\rho) + o(K).$$
Convergence for Large $K$

normalized delay cost
($\$/time \times \text{blocksize}$)

$\frac{\text{DelayCost}_K(\rho)}{K}$

$K = 20$
$K = 200$
$K = 2,000$
$K = 20,000$
$K \rightarrow \infty$

load $\rho$

0 0.1 0.2 0.3 0.4 0.5 0.6 0.7 0.8 0.9 1

0 1 2 3 4 5

Huberman, Leshno, Moallemi – Economic Analysis of Bitcoin
Convergence for Large $K$
Revenue and Delay for Small $\rho$

**Theorem:**
As $\rho \to 0$ we have that

$$\text{Rev}_\infty(\rho) = O\left(e^{-1/\rho}\right),$$
$$\text{DelayCost}_\infty(\rho) = \rho \cdot E[c] + o(\rho).$$

That is, delay costs are much larger than revenue for small $\rho$. 
Controlling Congestion – Revenue vs. Delay

![Graph showing the relationship between Revenue and Delay](image)

- $\text{Rev}_\infty(\rho)$ vs. $\text{DelayCost}_\infty(\rho)$
- Points indicating $\rho = 0.9$, $\rho = 0.95$, and $\rho = 0.975$

Huberman, Leshno, Moallemi – Economic Analysis of Bitcoin
Controlling Congestion with Different Maximal Block Size

![Graph showing Delay Cost vs Revenue with different maximal block sizes (K=20, K=200, K=2,000, K=20,000).]
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