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

Huberman, Leshno, Moallemi – Economic Analysis of Bitcoin
## 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="image1" 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="image2" 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="image3" alt="Graph" /></td>
</tr>
<tr>
<td>4</td>
<td>Ripple</td>
<td>$8,465,784,474</td>
<td>$0.220786</td>
<td>38,343,841,883 XRP*</td>
<td>$174,811,000</td>
<td>4.79%</td>
<td><img src="image4" 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="image5" 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="image6" 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="image7" 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="image8" alt="Graph" /></td>
</tr>
</tbody>
</table>


Huberman, Leshno, Moallemi – Economic Analysis of Bitcoin
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

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>Rules</td>
<td>Set by firm/org</td>
<td>Fixed by protocol</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>Procured by firm/org</td>
<td></td>
</tr>
<tr>
<td>Revenue</td>
<td>Fees set by firm/org</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 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>Revenue, entry/exit</td>
</tr>
<tr>
<td><strong>Revenue</strong></td>
<td>Fees set by firm/org</td>
<td>Equilibrium congestion pricing, all agents served</td>
</tr>
</tbody>
</table>

Huberman, Leshno, Moallemi – Economic Analysis of Bitcoin
Related Literature

- **Blockchain**

- **Usage of Bitcoin and the cryptocurrency market**

- **Queueing theory**
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

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

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

X 19.5 btc ➔ Y 3 btc
Z 16.4 btc
Fee 0.1 btc

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

Miner 1

Miner 2

Miner 7

mempool

Huberman, Leshno, Moallemi – Economic Analysis of Bitcoin
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

Huberman, Leshno, Moallemi – Economic Analysis of Bitcoin
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

Huberman, Leshno, Moallemi – Economic Analysis of Bitcoin
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)

Huberman, Leshno, Moallemi – Economic Analysis of Bitcoin
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 $\mu$
  - 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 $c \sim F[0, \bar{c}]$

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

- 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 $\frac{Rev}{N}$
- 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

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

Source: Croman et.al (2016)
Data: Miners Costs and Revenue Oct 2015

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

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

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

- Users play a congestion queueing game
  - Blocks mined/added at rate $\mu$, 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

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

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 $\mu$
- 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

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

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

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

where

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

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

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

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

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

Huberman, Leshno, Moallemi – Economic Analysis of Bitcoin
Expected Delay for Lowest Priority Transaction given Congestion $\rho$

Huberman,Leshno,Moallemi – Economic Analysis of Bitcoin
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 $K$.

\[
\text{Delay Costs} = K\rho \int_0^{\bar{c}} cf(c) \cdot W_K (\rho\bar{F}(c)) \, dc
\]

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

and

\[
N = \frac{Rev}{c_m}.
\]
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

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

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

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 $\Rightarrow$ No Revenues

- Low utilization $\rho$ 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 $\rho$
  - Bad dynamics, leads to system collapse

Huberman, Leshno, Moallemi – Economic Analysis of Bitcoin
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

Huberman, Leshno, Moallemi – Economic Analysis of Bitcoin
Design: Controlling $\mu$ and $K$

- Instead of having a fixed capacity, we consider adjusting $\mu$ 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.

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 $K$

![Graph showing normalized delay cost and load for different values of $K$. The x-axis represents load $\rho$, and the y-axis represents normalized delay cost $(\text{DelayCost}_K(\rho))/K$. The graph includes lines for $K = 20$, $K = 200$, $K = 2,000$, $K = 20,000$, and $K \to \infty$.](image-url)
Convergence for Large $K$

- $K = 20$
- $K = 200$
- $K = 2,000$
- $K = 20,000$
- $K \to \infty$
Revenue and Delay for Neglible Congestion

**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

$\text{DelayCost}_\infty(\rho) \quad (\$/\text{time} \times \text{blocksize})$

$\text{Rev}_\infty(\rho) \quad (\$/\text{time} \times \text{blocksize})$

- $\rho = 0.5$
- $\rho = 0.9$
- $\rho = 0.95$
- $\rho = 0.975$
Controlling Congestion

Huberman, Leshno, Moallemi – Economic Analysis of Bitcoin
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?

Huberman, Leshno, Moallemi – Economic Analysis of Bitcoin