Monopoly without a Monopolist: An Economic Analysis of the Bitcoin Payment System

Discussion: Igor Makarov

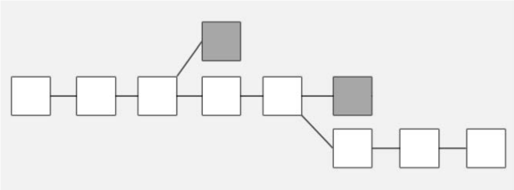
LSE

June 7, 2018

Motivation: blockchain

- Consider a typical transaction where a household pays a merchant with a debit/credit card
  - Processing and settlement is straightforward: the merchant contacts the issuing bank, the bank checks the balance, verifies the identity, and then approves/declines the transaction and updates the balance
  - Need to trust the bank, (and central bank)
- What if any given intermediary cannot be trusted?
  1. There is a predetermined set of agents who collectively are trustworthy
     - If the share of trusted agents > 2/3 the trust can be achieved using efficient Byzantine fault tolerant protocols
  2. There is no such a set $\Rightarrow$ blockchain (Satoshi Nakamoto (2008))
     - Cryptography + proof-of-work

Bitcoin Blockchain



- Transactions are assembled in blocks. Each block can have up to about 2K transactions
- Blocks form a chain: each block (except for the very first one) has one and only one block to which it is attached
- To have the right to attach the block one has to solve a difficult problem (a process called mining). The difficulty is adjusted over time so that on average it takes 10min to solve the puzzle
- Transactions included in a chain are deemed verified. The trust increases with the age of the block

Bitcoin Blockchain (cont.)

- The original design envisions many decentralized miners
- As long as 50% of miners are honest the blockchain is trusted
- With many miners, a successful attack requires a large amount of resources
- Miners are compensated for the resources spent in two ways:
  - Block reward
    - The block reward started at 50BTC
    - The block reward is halved every 210,000 blocks (currently 12.5BTC)
    - Theoretically this would lead to a maximum number of 21M BTC
  - Transaction fees (market price – current paper)

Why compensation for mining is important?

- Free-entry condition:

$$c_m \times N = \mathcal{R},$$

  - c_m – cost of mining a block
  - N – number of miners
  - $\mathcal{R}$ – Revenue per block = Block reward $+$ transaction fees

- If reward is small then the blockchain is vulnerable to an attack

Model

- Main insight: If there is no congestion, fees are small
- Queuing parameters:
  - Transactions arrive at Poisson rate λ
  - Blocks arrive at Poisson rate μ
  - Block size is K
  - $\Rightarrow$ Congestion: $\rho = \lambda / \mu K$
- The paper assumes that the current queue state is unobservable
- User i solves

$$\min_b b + c_i W(b, b_{-i}) \quad \Rightarrow \quad W'_b(b, b_{-i}) = \frac{1}{c_i}$$

  - c_i – cost of waiting (per unit of time), $c_i \sim F(\cdot)$
  - b – transaction fee
  - $W(b, b_{-i})$ – expected waiting time given b and fees of other agents b_{-i}

Equilibrium

- b in increasing in c_i
- Waiting time $W(b, b_{-i})$ is a function $\widehat{W}(\cdot)$ of $\bar{F}(c_i) \equiv 1 - F(c_i)$

$$W'_b(b, b_{-i}) = \widehat{W}'(\bar{F}(c_i)) \times f(c_i)/b'(c_i)$$

- Hence,

$$b(c_i) = \int_0^{c_i} c\widehat{W}'(\bar{F}(c_i))f(c)dc$$

⇒ User i pays the additional delay cost imposed on lower priority transactions

- Total fees per unit of time:

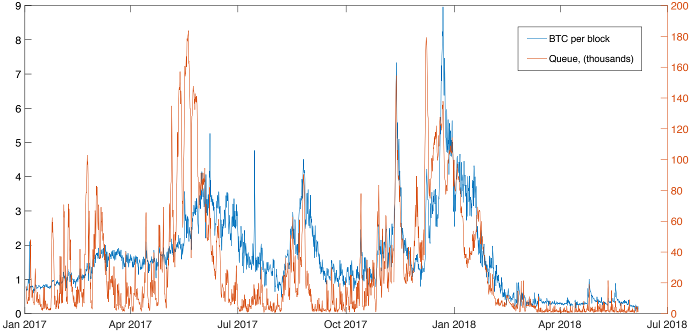
$$\lambda \int f(c)b(c)dc$$

Takeaways

- The model provides tools to compute miners' fees and the expected execution time as a function of Bitcoin payment system design
- Higher fees require higher delay in execution
- The results are useful for solving for the optimal design and thinking of viability of Bitcoin in the long run

Comments (1)

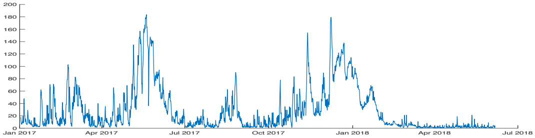
- The positive relationship between fees and the queue is a robust feature of the Bitcoin blockchain consistent with the model

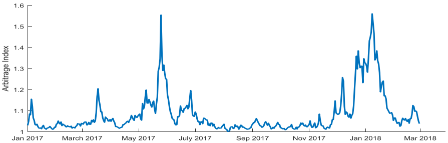


- In practice, the queue is observable and varies greatly over time ⇒ it would be interesting to know how it impacts the results

Comments (2)

- The variation in the queue seems to be linked to arbitrage opportunities in the Bitcoin market (Makarov and Schoar (2018))
  ⇒ λ and waiting cost might be correlated

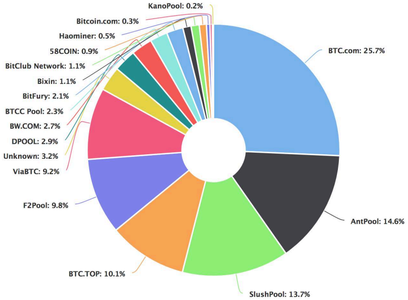




- It is likely that the future applications of Bitcoin, and hence the volume of transactions, will depend on the processing time of transactions and available alternatives

Comments (3)

- Reality of Bitcoin mining has diverged from the idealized design: Mining is dominated by few large mining pools (insurance motif)



- Implications:
  - Pools make profit ⇒ have stake in the continuation of the system
  - Pools have market power and so can dictate which transactions include into blocks

Comments (4)

- Having large mining pools means that the system depends on their objectives
- Their presence can contribute to the survival of the system (because they have a stake in it) but they can also co-opt the system for their own purposes
- Thus, the users de facto need to trust a predetermined set of agents
- These is at odds with the original design of Nakamoto
- Does not look very different from a traditional payment system with a few agents whom participants need to trust

Thank You!