# The Economic Limits of Bitcoin and the Blockchain

Author: E. Budish Discussant: D. Andolfatto

24th Annual Financial Markets Conference
FRB Atlanta, May 19-21, 2019

# Database management

- Information relating to individual action histories valued in society.
  - E.g., credit, education, performance histories.
- This information is used as a form of *currency*.
  - So, familiar incentives to counterfeit, fabricate, steal, etc.

# Database management

- Key Question: How are members of a community wanting to share and manage such information to do so when trust is lacking?

- Historically, small societies have relied on communal models, large societies on delegated models.
  - Small: recriprocal gift-exchange via "societal memory" (Kocherlakota).
  - Large: monetary exchange via centralized bank ledgers.

- Have innovations in electronic data storage, communications, cryptography, and game theory that make blockchain possible allow scaling of the communal model?

# What is a blockchain?

- A database management system with following properties:

  1. Hash-linked data structure with "open" read-privilege and permissionless access.

  2. Write-privilege determined by outcome of an "open" noncooperative game with no legal recourse.

- In contrast to conventional database management systems where:

  1. Data structures more general but with restricted-read privileges and permissioned access;

  2. Write-privilege restricted and delegated to legally liable third party.

## Why a blockchain?

- Conventional database management systems inherently more efficient.
  - E.g., compare *Fedwire* to *Bitcoin*.

- But blockchain may be preferred if delegated record-keeper is either...
  - Not trusted (e.g., Yahoo!, Equifax, banks).
  - Too expensive (e.g., Western Union).
  - Unavailable (e.g., firms in a supply chain).

# But can PoW-based blockchain scale?

- The hope for a very long time has been “yes.”

- Budish provides a compelling reason for why answer may be “no.”

## The argument

- Let $P =$ lottery prize, $N =$ lottery tickets sold, $c =$ cost per ticket.

- For given $(P, c)$, tickets sold $N^*$ satisfies $(1/N^*)P = c$.
  - So that $P = N^*c$ (total cost proportional to reward).

- For PoW, cost of majority-attack linear in $N^*c$.

- Let $V =$ value of majority-attack.

- Then, no-attack condition requires $\alpha N^*c > V$, or $\alpha P > V$.

# The argument

- What determines $V$?
  - The largest value transaction.
  - The value of sabotaging/shorting a competitor.
- $V$ could be very large! If so then condition $\alpha P > V$ implies a conundrum.
  - High $P$ required to secure largest possibly transaction, but increases cost of *all* transactions.
- Conventional database management systems (if well-designed) based on identifiable, legally-liable third parties, are less susceptible to this problem.

# Very interesting paper!

- Bitcoin code is open-source software–it evolves (code patches) over time.
  - Possible to make $P$ contingent on maximum transaction size (increase security when stakes are high)?
  - Possible that scaling occurs along extensive margin (forks)?

- Analysis seems targeted at PoW consensus protocols.
  - Is this a generic weakness in decentralized consensus mechanisms?
  - If so, is decentralized record-keeping doomed to fail?