Bitcoin's Fatal Flaw: The Limited Adoption Problem

Franz Hinzen
NYU Stern

Kose John
NYU Stern

Fahad Saleh
Wake Forest University

Research Question

Is Bitcoin’s underlying economic structure responsible for its limited adoption?

Key Take-Away

Research Question

Is Bitcoin’s underlying economic structure responsible for its limited adoption?

Key Take-Away

Yes!

Research Question

Is Bitcoin's underlying economic structure responsible for its limited adoption?

Key Take-Away

Yes!

Two Main Results:

- Limited Adoption I
  Bitcoin, as constructed, is subject to limited adoption.
- Limited Adoption II
  Allowing for variable transaction rates does not resolve the problem.

Limited Adoption I

- Increased usage leads to higher fees which induces increased mining activity
- Increased mining activity increases network delay, prolonging consensus
- Prolonged consensus yields prohibitive waits and thereby limited adoption

Limited Adoption I

- Increased usage leads to higher fees which induces increased mining activity
- Increased mining activity increases network delay, prolonging consensus
- Prolonged consensus yields prohibitive waits and thereby limited adoption

Limited Adoption II

- Increasing the transaction rate leads to persistent forks
- Persistent forks prolong consensus, yielding limited adoption

Limited Adoption I

- Increased usage leads to higher fees which induces increased mining activity
- Increased mining activity increases network delay, prolonging consensus
- Prolonged consensus yields prohibitive waits and thereby limited adoption

Limited Adoption II

- Increasing the transaction rate leads to persistent forks
- Persistent forks prolong consensus, yielding limited adoption

Our results are driven by the need for *consensus* and endogenous *network delay*.

Model Overview

Two Types of Agents

- Users
- Miners

Two Types of Payment Systems

- Bitcoin
- Traditional Alternative

Miners

A Miner refers to an individual processor

Miners (optimally) process fees in descending order

Mining sector is competitive so that:

$$\# \textit{ of Miners} \equiv M = \frac{\mathbb{E}[\sum f_i]}{\beta}$$

$\beta > 0$ denotes cost of a processor

f_i denotes User *i*'s equilibrium fee

Users

At $t = 0$, User i solves:

$$\max_{f \geqslant 0} R - \underbrace{c_i \cdot \mathbb{E}[W(f, f_{-i})]}_{\textit{Wait Disutility}} - \underbrace{f}_{\textit{Fee}}, \;\; c_i \sim U[0,1]$$

$W(f_i, f_{-i})$ denotes User i's wait time given that she pays fee f_i

Users

At $t = 0$, User i solves:

$$\max_{f \geqslant 0} R - \underbrace{c_i \cdot \mathbb{E}[W(f, f_{-i})]}_{\textit{Wait Disutility}} - \underbrace{f}_{\textit{Fee}}, \;\; c_i \sim U[0, 1]$$

$W(f_i, f_{-i})$ denotes User i's wait time given that she pays fee f_i

Outside Option
If $\max_{f_i \geqslant 0} R - c_i \cdot \mathbb{E}[W(f_i, f_{-i}) \mid c_i] - f_i < 0$ then User i does not transact via the blockchain

PoW Blockchain

A block is found when a miner solves a trivial puzzle.

Attempt to solve the puzzle equates mathematically to flipping a weighted coin.

Miners seek the puzzle solution via exhaustive enumeration.

A new block corresponds to a successful coin flip.

Poisson Limit Theorem

if $X_{i,n} \sim \mathit{Bernoulli}(p_n)$ i.d. and $\lim_{n \to \infty} n \times p_n = \lambda$ then

$$\sum_{i=1}^{n} X_{i,n} \xrightarrow{d} \mathit{Poisson}(\lambda)$$

PoW Blockchain (Continued)

An individual miner's block finding process is (approximately) Poisson.

Independent Poisson processes sum to a Poisson Process.

Previous papers assume network block production follows a Poisson process.

PoW Blockchain (Continued)

An individual miner's block finding process is (approximately) Poisson.

Independent Poisson processes sum to a Poisson Process.

Previous papers assume network block production follows a Poisson process.

... but network block production does not equal the sum of each miner's block production because forks exist!

Network delay may cause two blocks to be inconsistent with each other because PoW puzzles are a function of the history (i.e., forks).

We model **network delay**, allowing for disagreements arising from it.

Exponential Disagreement

Let $\Delta_i > 0$ denote the time taken to communicate one Tx to Node *i*.
Let $\lambda > 0$ denote the rate at which an ASIC finds puzzle solutions.

$$
\begin{aligned}
&\mathbb{P}\{\text{Agreement on a Block}\} \\
&= \prod_i \mathbb{P}\{\text{Time for Miner } i\text{'s Next Block} > \#\ Tx \times \Delta_i\} \\
&= \prod_i \exp\{-\lambda \times \#\ Tx \times \Delta_i\} \\
&= \exp\{-\Lambda \times \Delta\}
\end{aligned}
$$

Network Delay: $\Delta = \frac{1}{\#\ of\ Miners} \sum_i \Delta_i$
Blockchain Transaction Rate: $\Lambda = \lambda \times \#\ Tx \times \#\ of\ Miners$

Agreement probability decreases in Blockchain Transaction Rate, Λ.

Network Delay

We let $\Delta(M)$ denote the network delay of a network of size M.

Assumptions:

(1) $\Delta(1) = 0$

(2) $\lim_{M \to \infty} \Delta(M) = \infty$

(3) $\Delta'(M) > 0$

(1) holds by definition; (2) holds by physical limitations.

(3) holds for Bitcoin (see Chung and Lu 2002 and Riordan and Wormald 2010).

Equilibrium Conditions

- Users transact via the blockchain iff utility improving

$$\max_{f_i \geqslant 0} R - c_i \cdot \mathbb{E}[W(f_i, f_{-i})] - f_i \geqslant 0 \Leftrightarrow \forall i : c_i \leqslant c^*.$$

- Users select an optimal fee schedule

f_i solves $\max_{f_i \geqslant 0} R - c_i \cdot \mathbb{E}[W(f_i, f_{-i})] - f_i$ if $c_i \leqslant c^*$.
$f_i = 0$ otherwise.

- Miners earn no profits in equilibrium

$$\beta M = \mathbb{E}[\sum_i f_i].$$

Equilibrium: Existence and Uniqueness

Proposition

There exists an equilibrium. This equilibrium is unique among equilibria with differentiable fee functions that increase in wait disutility.

Note: This class of equilibria correspond to that studied by Huberman, Leshno and Moallemi (2019)

Limited Adoption I

Proposition

Bitcoin's adoption rate decreases as transaction demand rises (i.e., c^* decreases in N). Moreover, Bitcoin faces limited adoption (i.e., $\lim_{N \to \infty} c^* = 0$).

Proposition

The adoption rate for Bitcoin is lower than that of an alternative system without endogenous network delay for large transaction demands.

LAP I Intuition

The marginal user, c^*, earns zero utility from Bitcoin:

$$\underbrace{R}_{\textit{Exogenous Utility}} = \underbrace{c^*\Psi(\Lambda, M)}_{\textit{Wait Disutility}} + \underbrace{\frac{(c^*)^2(N-1)}{2\Lambda}}_{\textit{Fee}}$$

LAP I Intuition

The marginal user, c^*, earns zero utility from Bitcoin:

$$\underbrace{R}_{\textit{Exogenous Utility}} = \underbrace{c^*\Psi(\Lambda, M)}_{\textit{Wait Disutility}} + \underbrace{\frac{(c^*)^2(N-1)}{2\Lambda}}_{\textit{Fee}}$$

- Increased usage induces increased mining activity ($N \uparrow \implies M \uparrow$)
- Increased mining activity increases network delay ($M \uparrow \implies \Delta(M) \uparrow$)
- Increased network delay prolongs consensus ($\Delta(M) \uparrow \implies \Psi(\Lambda, M) \uparrow$)
- Consequently, Limited Adoption arises ($c^* \searrow 0$)

Limited Adoption II

Proposition

Suppose that Bitcoin's transaction rate, Λ_N, varies with transaction demand, N. Then, as long as Bitcoin remains decentralized, Bitcoin necessarily experiences limited adoption $(\text{i.e., } \lim_{N \to \infty} c^* = 0)$.

LAP II Intuition

Expected Wait Time

= Expected Traditional Wait Time + Expected Consensus Wait Time

$$= \frac{\mathbb{E}[\# \textit{Higher Priority Users}]}{\Lambda} +$$

Traditional wait decreases in blockchain transaction rate, Λ.

LAP II Intuition

Expected Wait Time

= Expected Traditional Wait Time + Expected Consensus Wait Time

$$= \frac{\mathbb{E}[\#\textit{Higher Priority Users}]}{\Lambda} + \frac{\exp\{\Lambda \times \Delta\} - 1}{\Lambda}$$

Traditional wait decreases in blockchain transaction rate, Λ.

... but consensus wait diverges with transaction rate. (i.e., $\lim_{\Lambda \to \infty} \frac{\exp\{\Lambda \times \Delta\} - 1}{\Lambda} = \infty$)

Counterfactual: No Network Delay

Network delay, an attribute of a distributed system and therefore a blockchain, serves as a critical factor for the results.

Absent network delay, the traditional solution of expanding supply to meet demand resolves the problem.

Proposition

Both widespread adoption (i.e., $c^* \to \underline{c} > 0$) and decentralization (i.e., $M \to \infty$) can be obtained simultaneously under the counterfactual assumption of no network delay (i.e., $\Delta(M) = 0$).

Conclusion

- Limited Adoption is endemic to Bitcoin.
- The traditional solution (i.e., expanding supply to meet demand) fails.
- More research is needed on alternatives...