Bitcoin's Fatal Flaw: The Limited Adoption Problem

Franz Hinzen
NYU Stern

Kose John
NYU Stern

Fahad Saleh
McGill Desautels

10 Years after inception, Bitcoin remains sparsely adopted.

Does that fact arise from Bitcoin's infancy or structure?

"We demonstrate that the economics of [Bitcoin] make limited adoption an inescapable equilibrium outcome."

10 Years after inception, Bitcoin remains sparsely adopted.

Does that fact arise from Bitcoin's infancy or structure?

"We demonstrate that the economics of [Bitcoin] make limited adoption an inescapable equilibrium outcome."

Economic Channel: Negative Network Effects

Blockchain 101

- Electronic Ledger
  - Entries are recorded in discrete chunks called blocks
  - Blocks are chained together in a near-chronological order

Blockchain 101

- Electronic Ledger
  - Entries are recorded in discrete chunks called blocks
  - Blocks are chained together in a near-chronological order
- Distributed System
  - Network of agents
  - Each agent holds a copy of the ledger

Blockchain 101

- Electronic Ledger
  - Entries are recorded in discrete chunks called blocks
  - Blocks are chained together in a near-chronological order
- Distributed System
  - Network of agents
  - Each agent holds a copy of the ledger

Consensus: The network must agree on ledger contents

... that introduces a technical constraint (network delay)

Network delay contributes to negative network effects.

An Adoption Problem

Bitcoin possesses three key features:

- need for agreement on ledger contents (consensus)

An Adoption Problem

Bitcoin possesses three key features:

- need for agreement on ledger contents (consensus)
- free entry (aka permissionless, “decentralized”)

An Adoption Problem

Bitcoin possesses three key features:

- need for agreement on ledger contents (consensus)
- free entry (aka permissionless, “decentralized”)
- artificial supply constraint (BTC: $\approx$10 minute block times)

These features generate limited adoption.

An Adoption Problem: Economic Channel

Bitcoin imposes an artificial supply constraint

Thus, positive demand shocks induce a price increase (fees ↑)

An Adoption Problem: Economic Channel

Bitcoin imposes an artificial supply constraint

Thus, positive demand shocks induce a price increase (fees ↑)

Fee increases expand the validator network (free entry)

An Adoption Problem: Economic Channel

Bitcoin imposes an artificial supply constraint

Thus, positive demand shocks induce a price increase (fees ↑)

Fee increases expand the validator network (free entry)

Expanded network protracts consensus process

Prohibitive wait times result

Payment system viability relies on speed, so limited adoption arises

Fixed Supply + Free Entry + Consensus = Limited Adoption

Decentralization implies Limited Adoption

Note: The aforementioned problem is artificial!
i.e., block times are artificially constrained.

One putative solution: Relax the artificial supply constraint
i.e., Let block times vary with demand

Decentralization implies Limited Adoption

Note: The aforementioned problem is artificial!
i.e., block times are artificially constrained.

One putative solution: Relax the artificial supply constraint
i.e., Let block times vary with demand

Drawback: This solution succeeds only insofar as it induces centralization!

Arbitrarily fast block times cause delays to diverge purely due to the consensus process

Thus, even with dynamic block times, limited adoption obtains!

A Solution: Public Permissioned Blockchain

A permissioned blockchain overcomes limited adoption by forgoing both free entry and fixed supply

Validator incentives, however, become relevant

Traditional voting schemes generate a co-ordination game with multiple equilibria, some undesirable

A stake-based voting scheme overcomes the limited adoption problem while precluding a bad co-ordination equilibrium

Related Literature

Economic Limitations of Bitcoin

Yermack (2015); Budish (2018); Biais, Bisiere, Bouvard, and Casamatta (2019); Foley, Hinzen, John and Saleh (2019); Saleh (2019b)

Alternative Protocols

Bentov, Pass and Shi (2016); Chen and Micali (2016); Hinzen, Irresberger, John and Saleh (2019); Rosu and Saleh (2019); Russell, David, and Oliynykov (2017); Saleh (2019a)

Tokenomics

Chod and Lyandres (2019); Cong and He (2019); Cong, Li and Wang (2019a); Cong, Li and Wang (2019b); Howell, Niessner, and Yermack (2019); Lee, Li, and Shin (2019); Lyandres (2019); Lyandres, Palazzo, and Rabetti (2019)

Overview

Two Types of Agents

- Validators (i.e., Miners)
- Users

Two Types of Payment Systems

- Bitcoin
- Traditional Alternative

Validators

Validators reference individual processors

Validators

Validators reference individual processors

Validators (optimally) process fees in descending order

Validator sector is competitive so that:

$$V = \frac{\mathbb{E}[\sum f_i]}{\beta}$$

$\beta > 0$ denotes cost of a processor

Users

User i receives utility $R > 0$ if her transaction confirms

User i dislikes waiting and has time-sensitivity $c_i \sim U[0, 1]$

User i dislikes having to pay a fee for processing

User Problem

At $t = 0$, User i solves:

$$\max_{f_i \geqslant 0} R - c_i \cdot \mathbb{E}[W(f_i, f_{-i}) \mid c_i] - f_i$$

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

User Problem

At $t = 0$, User i solves:

$$\max_{f_i \geqslant 0} R - c_i \cdot \mathbb{E}[W(f_i, f_{-i}) \mid c_i] - f_i$$

$W(f_i, f_{-i})$ 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

Blockchain

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

Validators seek the puzzle solution via exhaustive enumeration.

Blockchain

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

Validators seek the puzzle solution via exhaustive enumeration.

Validator behavior maps to Bernoulli trials.

A valid block maps to a successful Bernouli trial.

Blockchain

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

Validators seek the puzzle solution via exhaustive enumeration.

Validator behavior maps to Bernoulli trials.

A valid block maps to a successful Bernouli trial.

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

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

Blockchain (Continued)

A validator's block finding process is (approximately) Poisson.

Independent Poisson processes sum to a Poisson Process.

Previous papers assume blocks arrive according to a Poisson process.

Blockchain (Continued)

A validator's block finding process is (approximately) Poisson.

Independent Poisson processes sum to a Poisson Process.

Previous papers assume blocks arrive according to a Poisson process.

This aggregation neglects network delay.

We augment that model to allow that disagreements arise from network delay.

Decker and Wattenhofer (2013) demonstrates that most Bitcoin disagreements arise precisely due to network delay.

Blockchain (Continued)

Disagreement occurs if one validator finds a block and then some other validator finds a block before hearing about the first block.

Note: Poisson arrivals are exponentially distributed.

Blockchain (Continued)

Disagreement occurs if one validator finds a block and then some other validator finds a block before hearing about the first block.

Note: Poisson arrivals are exponentially distributed.

$$p \equiv \mathbb{P}\{\text{No Disagreement}\} = \prod_i e^{-\lambda \Delta_i} = e^{-\Lambda \Delta}$$

with $\Delta = \frac{1}{V} \sum_i \Delta_i$ and $\Lambda = \lambda V$

Network Delay

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

Assumptions:

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

Network Delay

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

Assumptions:

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

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

Network Delay

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

Assumptions:

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

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

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

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

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

Equilibrium Conditions

- Users transact via the blockchain iff utility improving

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

Equilibrium Conditions

- Users transact via the blockchain iff utility improving

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

- Users select an optimal fee schedule

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

Equilibrium Conditions

- Users transact via the blockchain iff utility improving

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

- Users select an optimal fee schedule

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

- Validators earn no profits in equilibrium

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

Equilibrium: Existence and Uniqueness

Proposition

There exists an equilibrium. This equilibrium is unique among equilibrium with fee functions differentiable and increasing in wait dis-utility.

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

Demand and Validator Network Size

Increased Demand induces Higher Fees

Higher fees induce Validator Entry

More Formally,

Lemma

V increases in N and $\lim_{N \to \infty} V_N = \infty$

Expected Wait Time Decomposition

$$W_i = \frac{1}{\Lambda} + (N-1)\frac{(c^* - c_i)}{\Lambda} + \tau(\Lambda, V)$$

$\frac{1}{\Lambda}$ denotes expected personal service time

Expected Wait Time Decomposition

$$W_i = \frac{1}{\Lambda} + (N-1)\frac{(c^* - c_i)}{\Lambda} + \tau(\Lambda, V)$$

$\frac{1}{\Lambda}$ denotes expected personal service time

$(N-1)\frac{(c^* - c_i)}{\Lambda}$ denotes expected wait for higher-priority users

Expected Wait Time Decomposition

$$W_i = \frac{1}{\Lambda} + (N-1)\frac{(c^* - c_i)}{\Lambda} + \tau(\Lambda, V)$$

$\frac{1}{\Lambda}$ denotes expected personal service time

$(N-1)\frac{(c^* - c_i)}{\Lambda}$ denotes expected wait for higher-priority users

$\tau(\Lambda, V)$ denotes expected disagreement resolution time

Expected Wait Time Divergence

Increased demand leads to a more dispersed validator network. The more dispersed validator network induces more frequent disagreement. These disagreements delay consensus. In fact,

$$\lim_{N\to\infty} \tau(\Lambda, V_N) = \infty$$

Waits diverge even for the highest priority users!

$$\lim_{N\to\infty} \inf_i W_i = \infty$$

An Adoption Problem

Proposition

Adoption decreases as demand rises (i.e., c^* decreases in N). Moreover, the blockchain faces limited adoption (i.e., $c^* \to 0$).

An Adoption Problem

Proposition

Adoption decreases as demand rises (i.e., c^* decreases in N). Moreover, the blockchain faces limited adoption (i.e., $c^* \to 0$).

Increased Demand
$\Longrightarrow$ Increased Fees
$\Longrightarrow$ Larger Validator Network
$\Longrightarrow$ Protracted Consensus Process
$\Longrightarrow$ Prohibitive Delays
$\Longrightarrow$ Limited Adoption

Decentralization implies Limited Adoption

Why not relax the artificial supply constraint? (i.e., increase Λ with N)

Decentralization implies Limited Adoption

Why not relax the artificial supply constraint? (i.e., increase Λ with N)

Even with a small network size, fast block times make consensus resolution diverge

Limited Adoption is overcome only if the network becomes centralized.

Proposition

The blockchain necessarily faces either centralization (i.e., $V \to 1$) or limited adoption (i.e., $c^* \to 0$).

Faster Blocks vs. More Disagreement

Speeding up the blockchain produces blocks faster but these blocks are also more likely to yield disagreement.

Faster Blocks vs. More Disagreement

Speeding up the blockchain produces blocks faster but these blocks are also more likely to yield disagreement.

Within Bitcoin's protocol, speeding up the blockchain produces exponentially more disagreement.

As such, speeding up the blockchain eventually increases wait-times and cannot overcome limited adoption without centralization

Exponential Disagreement

Recall that agreement occurs with probability $p = e^{-\Lambda\Delta}$

Thus, the likelihood of agreement decays exponentially in the block rate.

Exponential Disagreement

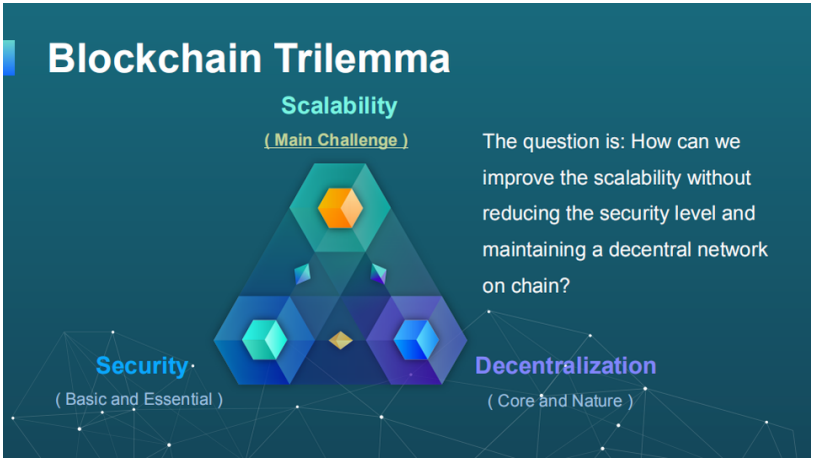
Recall that agreement occurs with probability $p = e^{-\Lambda\Delta}$

Thus, the likelihood of agreement decays exponentially in the block rate.

Expected Time to a Disagreement-Free Block:

$$\frac{1}{p \times \Lambda} = \frac{e^{\Lambda\Delta}}{\Lambda} \to \infty \text{ as } \Lambda \to \infty$$

Buterin's Trilemma



Significance of 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., $V \to \infty$) can be obtained simultaneously under the counterfactual assumption of no network delay (i.e., $\Delta(V) = 0$).

(Public) Permissioned Blockchain

Permissioned blockchains differ from Bitcoin by specifying a fixed set of validators. (i.e., no free entry)

This reduces the significance of network delay.

(Public) Permissioned Blockchain

Permissioned blockchains differ from Bitcoin by specifying a fixed set of validators. (i.e., no free entry)

This reduces the significance of network delay.

Permissioned Blockchains also remove the need for the Bitcoin puzzle which reduces wait times.

Proposition

In any Permissioned Equilibrium, widespread adoption (i.e., $c^* \to \underline{c} > 0$) obtains.

A Different Problem

Obtaining adoption for a permissioned blockchain is easy.

... but the purported advantage of Bitcoin-style blockchains is security not adoption.

Thus, the question becomes: are permissioned blockchains secure?

A Different Problem

Obtaining adoption for a permissioned blockchain is easy.

... but the purported advantage of Bitcoin-style blockchains is security not adoption.

Thus, the question becomes: are permissioned blockchains secure?

This Paper: In general, No.

Aside: Where's the Blockchain?

Digital Signatures

- A valid block must be digitally signed by validators
- This creates accountability

Aside: Where's the Blockchain?

Digital Signatures

- A valid block must be digitally signed by validators
- This creates accountability

Hash-Linking

- The data structure uses hash-linking.
- Hash-linking makes fraud detection trivial.

Aside: Where's the Blockchain?

Digital Signatures

- A valid block must be digitally signed by validators
- This creates accountability

Hash-Linking

- The data structure uses hash-linking.
- Hash-linking makes fraud detection trivial.

Validator identity is known, so reputation is particularly important.

Equilibrium

V_3 plays H

V_1 \ V_2	H	M
H	$(0, 0, 0)$	$(0, -\kappa, 0)$
M	$(-\kappa, 0, 0)$	$(\Pi, \Pi, 0)$

V_3 plays M

V_1 \ V_2	H	M
H	$(0, 0, -\kappa)$	$(0, \Pi, \Pi)$
M	$(0, \Pi, \Pi)$	(Π, Π, Π)

$\kappa > 0$ represents a reputation cost.

$\Pi > 0$ represents a profit from malicious behavior.

H (M) represents Honest (Malicious) behavior.

Stake-based Permissioned Blockchain

We propose that blocks are selected based on a weighted vote among validators with weights being holdings in the native cryptocurrency.

Stake-based Permissioned Blockchain

We propose that blocks are selected based on a weighted vote among validators with weights being holdings in the native cryptocurrency.

Malicious behavior erodes value of cryptocurrency.

Cryptocurrency holding is endogenous.

Stake-based Permissioned Blockchain

We propose that blocks are selected based on a weighted vote among validators with weights being holdings in the native cryptocurrency.

Malicious behavior erodes value of cryptocurrency.

Cryptocurrency holding is endogenous.

Proposition

There exists no equilibrium in which an attack succeeds with strictly positive probability.

Aside: Not Proof-of-Stake (PoS)

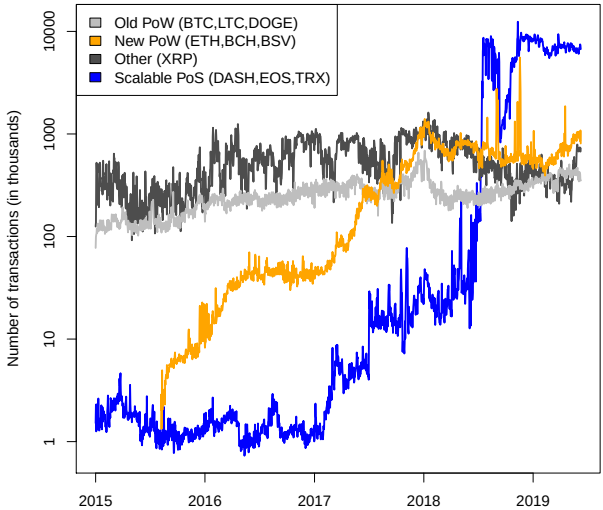
PoS allows any agent to participate in the validation process and therefore is permissionless.

Our proposed rule weights votes only among a specified permissioned set.

Our setting is permissioned with transparent identity - this creates an additional disincentive for malicious behavior arising from reputation costs.

Conclusion

- Limited Adoption is endemic to Bitcoin.
- The traditional solution (i.e., increasing throughput) fails.
- More research is needed on alternatives...



Source: Hinzen, Irresberger, John and Saleh (2019)