Bitcoin’s Fatal Flaw: The Limited Adoption Problem

Franz Hinzen, Kose John, Fahad Saleh

Discussion by Katya Malinova
Brief Summary

- Blockchain as payment infrastructure
Brief Summary

- Blockchain as payment infrastructure

- Bitcoin (proof-of-work) blockchain is not scalable
  - Limited adoption: the fraction of users who use the blockchain for payments vanishes as the number of users increases
Brief Summary

- Blockchain as payment infrastructure

- Bitcoin (proof-of-work) blockchain is not scalable
  - Limited adoption: the fraction of users who use the blockchain for payments vanishes as the number of users increases

- Permissioned blockchain is a viable alternative
  - But not for all consensus mechanisms, e.g.:
    - simple majority voting doesn't work
    - voting scaled by crypto-currency holdings does
Model (PoW): Users
Model (PoW): Users

N users need to transact & choose:
Model (PoW): Users

N users need to transact & choose:

Blockchain:
Model (PoW): Users

N users need to transact & choose:

Blockchain:

\[
\max_{f_i \geq 0} R - c_i \cdot \mathbb{E}[W(f_i, f_{-i}) | c_i] - f_i
\]
Model (PoW): Users

N users need to transact & choose:

Blockchain:

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

Reward (from using blockchain?)
Model (PoW): Users

N users need to transact & choose:

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

Blockchain:

Reward (from using blockchain?)

Fee to miners
Model (PoW): Users

N users need to transact and choose:

Blockchain:

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

- **Reward** (from using blockchain?)
- **Waiting cost:** "user impatience \(c_i\)" × "time to confirm"
- **Fee to miners**
Model (PoW): Users

N users need to transact & choose:

Blockchain:

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

Reward (from using blockchain?)

Waiting cost: "user impatience $c_i$" \times "time to confirm"

Fee to miners

"Traditional" payment system
- unmodelled
- normalized as zero reward, zero cost?
Model (PoW): Validators
Model (PoW): Validators

- Assumed to coordinate on the longest chain, no malicious behavior
Model (PoW): Validators

- Assumed to coordinate on the longest chain, no malicious behavior

- Free entry:
Model (PoW): Validators

- Assumed to coordinate on the longest chain, no malicious behavior
- Free entry:

\[ V = \frac{E[\sum f_i]}{\beta} \]
Model (PoW): Validators

- Assumed to coordinate on the longest chain, no malicious behavior
- Free entry:

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

Number of validators

Sum of user fees
Model (PoW): Validators

- Assumed to coordinate on the longest chain, no malicious behavior

- Free entry:

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

Number of validators

Cost of validation technology

Sum of user fees
Model (PoW): Equilibrium
Model (PoW): Equilibrium

- Low enough impatience $c_i \leq c^*$ ⇒ use blockchain
- Marginal user $c^*$ pays the highest fee and waits for:
Model (PoW): Equilibrium

- Low enough impatience $c_i \leq c^* \Rightarrow$ use blockchain
- Marginal user $c^*$ pays the highest fee and waits for:

$$\frac{1}{\Lambda} + \tau(\Lambda, V)$$
Model (PoW): Equilibrium

- Low enough impatience $c_i \leq c^* \Rightarrow$ use blockchain
- Marginal user $c^*$ pays the highest fee and waits for:

$$\frac{1}{\Lambda} + \tau(\Lambda, V)$$

block's arrival rate
Model (PoW): Equilibrium

- Low enough impatience $c_i \leq c^*$ ⇒ use blockchain
- Marginal user $c^*$ pays the highest fee and waits for:

$$\frac{1}{\Lambda} + \tau(\Lambda, V)$$

- block's arrival rate
- fork/dispute resolution time
Model (PoW): Equilibrium

- Low enough impatience $c_i \leq c^* \Rightarrow$ use blockchain
- Marginal user $c^*$ pays the highest fee and waits for:

\[
\frac{1}{\Lambda} + \tau(\Lambda, V)
\]

- block's arrival rate
- fork/dispute resolution time
Model (PoW): Equilibrium

- Low enough impatience $c_i \leq c^*$ ⇒ use blockchain
- Marginal user $c^*$ pays the highest fee and waits for:

\[
\frac{1}{\Lambda} + \tau(\Lambda, V) \rightarrow \infty \quad \text{as } N \rightarrow \infty
\]
Model (PoW): Equilibrium

- Low enough impatience $c_i \leq c^*$ ⇒ use blockchain
- Marginal user $c^*$ pays the highest fee and waits for:

\[
\frac{1}{\Lambda} + \tau(\Lambda, V) = \infty \quad \text{as} \quad N \to \infty
\]

$c^* \to 0$

"limited adoption"
\[ \frac{1}{A} + \tau(A, V) \]
Comments/Questions:

- Why do forks take \( \infty \) to resolve?
Comments/Questions:

- Why do forks take $\infty$ to resolve?

Key Result:

- as $N \to \infty$, the number of validators $V \to \infty$
Comments/Questions:

• Why do forks take $\infty$ to resolve?

Key Result:

• as $N \rightarrow \infty$, the number of validators $V \rightarrow \infty$

Network delay/physical system limits

• $\rightarrow$ with $V = \infty$, time to agree/communicate explodes
Comments/Questions:

- Why do forks take $\infty$ to resolve?

Key Result:

- as $\mathcal{N} \to \infty$, the number of validators $V \to \infty$

Network delay/physical system limits

- $\to$ with $V = \infty$, time to agree/communicate explodes

Lemma B.1 in Appendix B....
Number of validators $V$ determined by free entry:
Number of validators $V$ determined by free entry:

$$V = \frac{E[\sum f_i]}{\beta}$$
Number of validators $V$ determined by free entry:

$$V = E[\sum_{\beta} f_i]$$
Number of validators $V$ determined by free entry:

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

Number of users $N \to \infty$

$\implies$ expected fees $\to \infty$
Number of validators $V$ determined by free entry:

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

Number of users $N \rightarrow \infty$

- $\Rightarrow$ expected fees $\rightarrow \infty$

Comment 1: need more intuition for this:

- User $i$ pays fee $f_i \propto (N - 1)c_i^2$
- With $N \rightarrow \infty$, wait times explode & only super-patient users use blockchain ....
  - $\Rightarrow c_i \approx 0$
- Fraction of blockchain users vanishes ...
- What happens to fee per user?

$$f \propto i \left( N - 1 \right) c_i^2$$
Comments/Questions:

Number of validators $V$ determined by free entry:

$$V = \frac{\mathbb{E} \left[ \sum_{\beta} f_i \right]}{\mathbb{E} \left[ \sum_{\beta} f_i \right]}$$

Number of users $N \rightarrow \infty$

• $\Rightarrow$ expected fees $\rightarrow \infty$
Number of validators $V$ determined by free entry:

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

Number of users $N \to \infty$
- $\Rightarrow$ expected fees $\to \infty$

Comment 2:
- Confirmation times $\to \infty$
  $\Rightarrow$ fees are received with infinite delay
- Technology costs are incurred in real time! (?)
- Are validators infinitely patient? No capital constraints?
  - Is there a transversality condition?
Model 2: (Permissioned Blockchain)

Users:
- same as before

Validators:
- Finite number
- Play a coordination game, choose:
  - be malicious
    - exogenous reward & cost
  - be honest
Model 2: (Permissioned Blockchain)

Users:
- same as before

Validators:
- Finite number
- Play a coordination game, choose:
  - be malicious
    - exogenous reward & cost
  - be honest

Where does the reward come from?
Seemingly should depend on the value of transactions and/or malicious users?
Suggestion: One Paper, One Model
This paper: 2.5 models

1. Proof-of-Work -- validators' incentives unmodelled
2. Permissioned -- coordination game among validators
   • with majority voting
   • with crypto-currency stake-weighted voting
     → must introduce and value cryptocurrency
Suggestion: One Paper, One Model

This paper: 2.5 models

1. Proof-of-Work -- validators' incentives unmodelled
2. Permissioned -- coordination game among validators
   - with majority voting
   - with crypto-currency stake-weighted voting
     - must introduce and value cryptocurrency

No clear connection between #1 and #2

- Why move from decentralized proof-of-work to permissioned?
- Are there decentralized alternatives?
  - E.g., require minimum crypto-stake to become a validator?
Question: purpose of a blockchain in the model?
Users obtain a reward from transacting on the blockchain:

- similar reward structure for permissionless PoW vs. permissioned
Question: purpose of a blockchain in the model?

Users obtain a reward from transacting on the blockchain:
- similar reward structure for permissionless PoW vs. permissioned

Where does the utility gain from blockchain use stem from?
- E.g., with bitcoin: censorship-resistance, immutability ...
- But this disappears if blockchain is permissioned
Question: purpose of a blockchain in the model?

Users obtain a reward from transacting on the blockchain:
- similar reward structure for permissionless PoW vs. permissioned

Where does the utility gain from blockchain use stem from?
- E.g., with bitcoin: censorship-resistance, immutability ...
- But this disappears if blockchain is permissioned

Key differences (from the user perspective) b/n the permissioned blockchain vs. traditional payment system in the model?
- Central Bank Digital Currency?
Various "impossibility triangles" have been discussed:

- The authors mention Buterin's: scalability, security, decentralization triangle
- This is also discussed in the academic literature, e.g.:
  - econ&finance: Abadi and Brunermeier (2018)
  - see Chen, Cong, Xiao (2019) for a survey
The paper:
- co-existence of payment and currency systems
- role for the value of cryptocurrency (for the voting weights)
- users don't directly affect crypto-valuation

Is this approach consistent with the predictions from the user-driven cryptocurrency valuation models, where value is affected by e.g.:
- possible speculation
- coordination among users
- see Malinova (2019) for a survey