Federal Reserve Bank of Philadelphia

Third Annual Fintech Conference

November 14–15, 2019

Bitcoin's Fatal Flaw: The Limited Adoption Problem

Franz Hinzen, Kose John, Fahad Saleh

Discussion by Katya Malinova

BRIGHTER WORLD

DeGroote
SCHOOL OF BUSINESS
EDUCATION WITH PURPOSE

McMaster University

Brief Summary

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

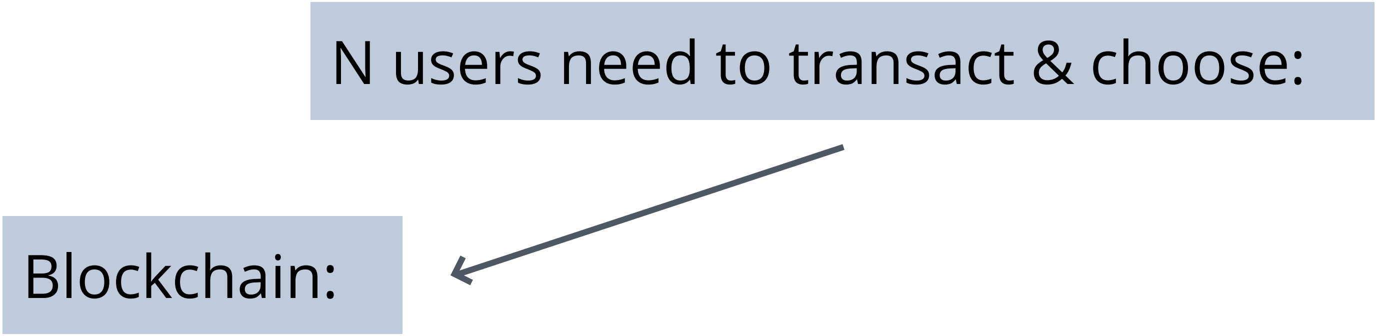
- Permissioned blockchain is a viable alternative
  - But not for all consensus mechanisms, e.g.:
    - simple majority voting doesn't work
    - voting scaled by crypto-currency holdings does

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:

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

Model (PoW): Users

N users need to transact & choose:

Blockchain:

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

Reward (from using blockchain?)

Model (PoW): Users

N users need to transact & choose:

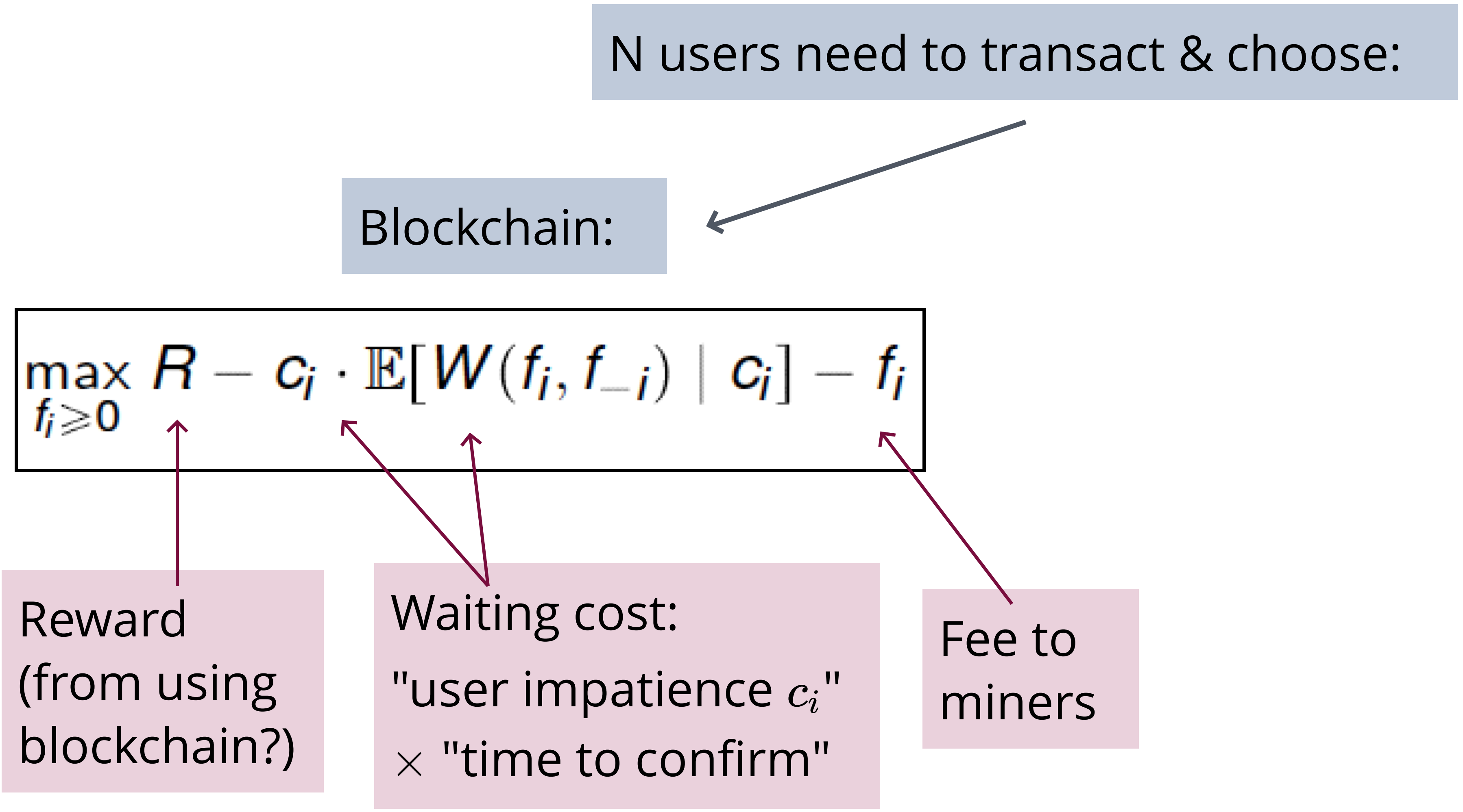
Blockchain:

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

Reward (from using blockchain?)

Fee to miners

Model (PoW): Users



N users need to transact & choose:

Blockchain:

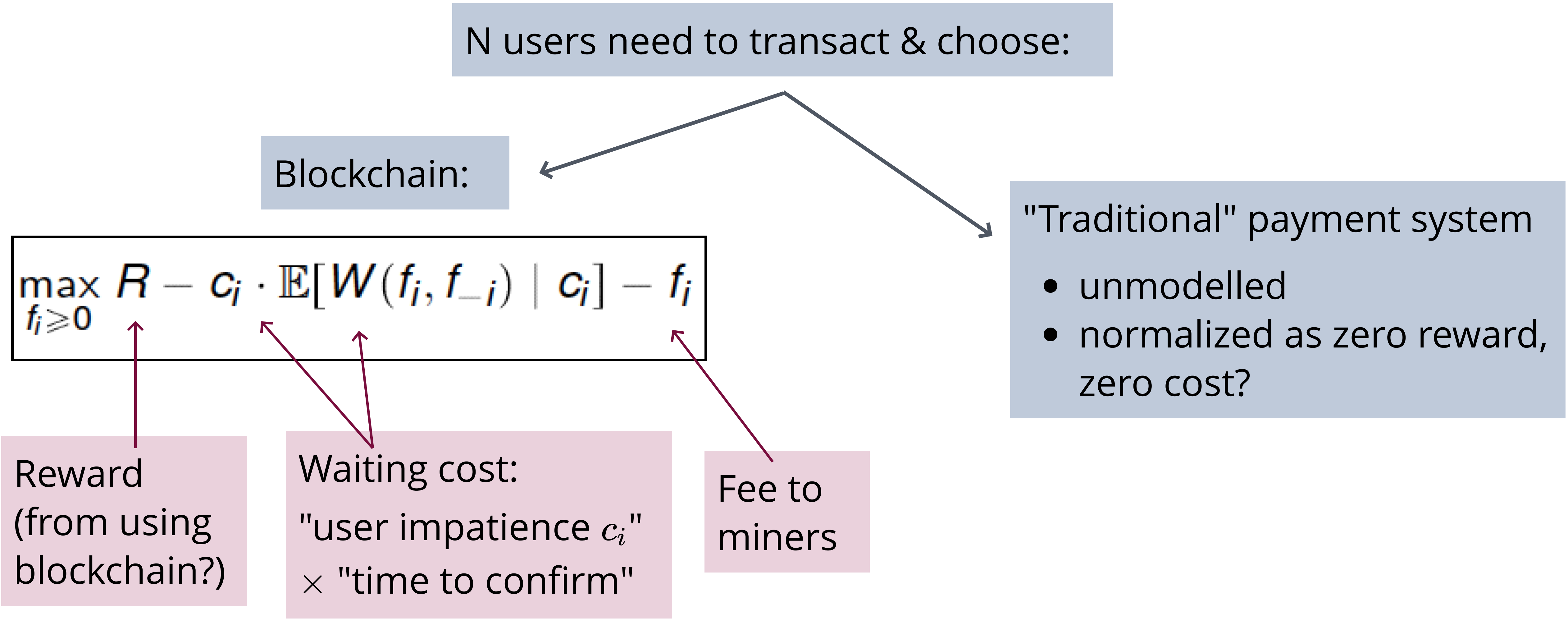
$$\max_{f_i \geqslant 0} R - c_i \cdot \mathbb{E}[W(f_i, f_{-i}) \mid c_i] - f_i$$

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:

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

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:

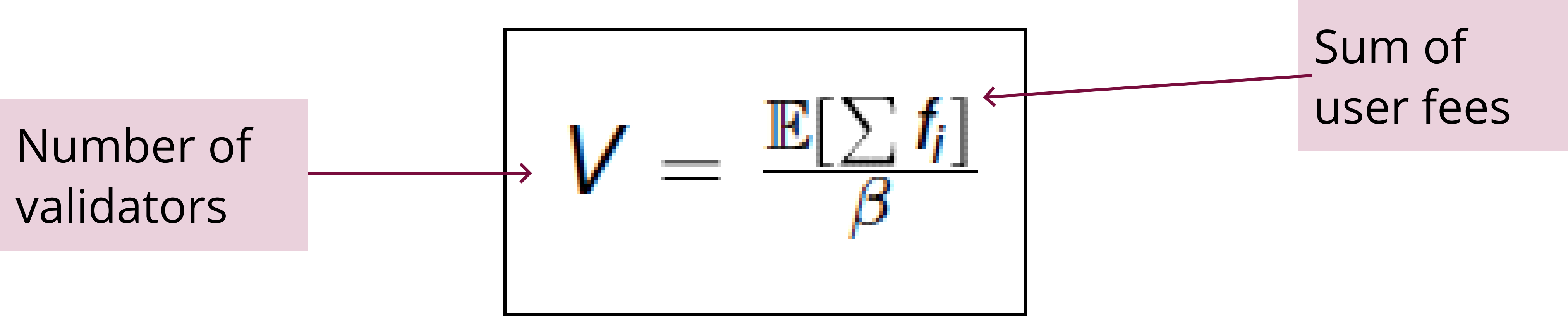
Number of validators

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

Model (PoW): Validators

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

- Free entry:



Number of validators

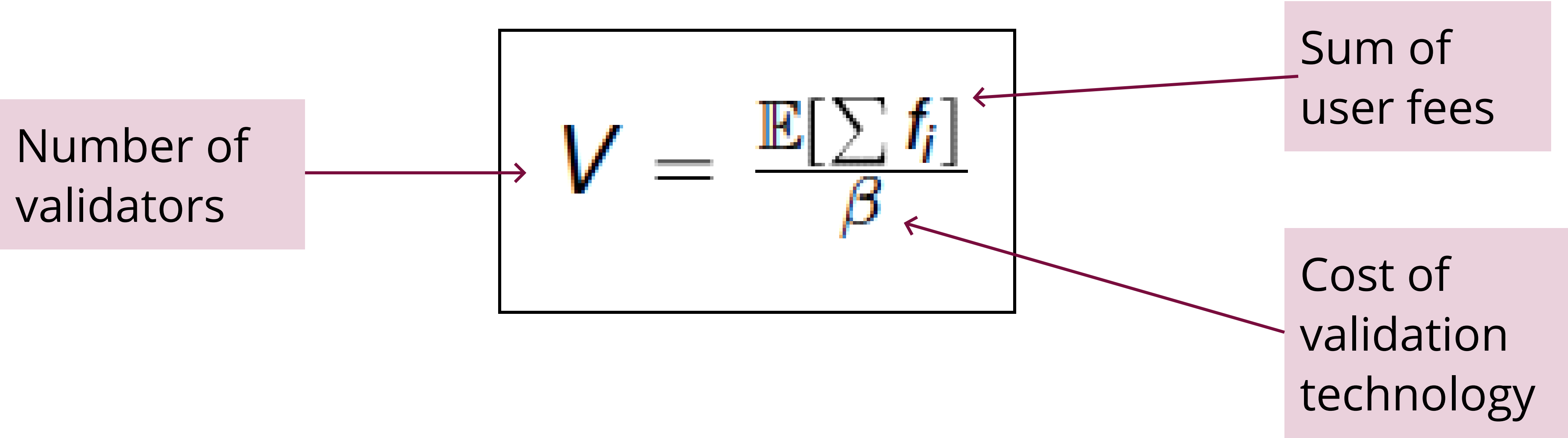
$$V = \frac{\mathbb{E}[\sum f_i]}{\beta}$$

Sum of user fees

Model (PoW): Validators

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

- Free entry:



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

Number of validators

Sum of user fees

Cost of validation technology

Model (PoW): Equilibrium

Model (PoW): Equilibrium

- Low enough impatience $c_i \leq c^* \Rightarrow$ 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:

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

Model (PoW): Equilibrium

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

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

block's arrival rate

Model (PoW): Equilibrium

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

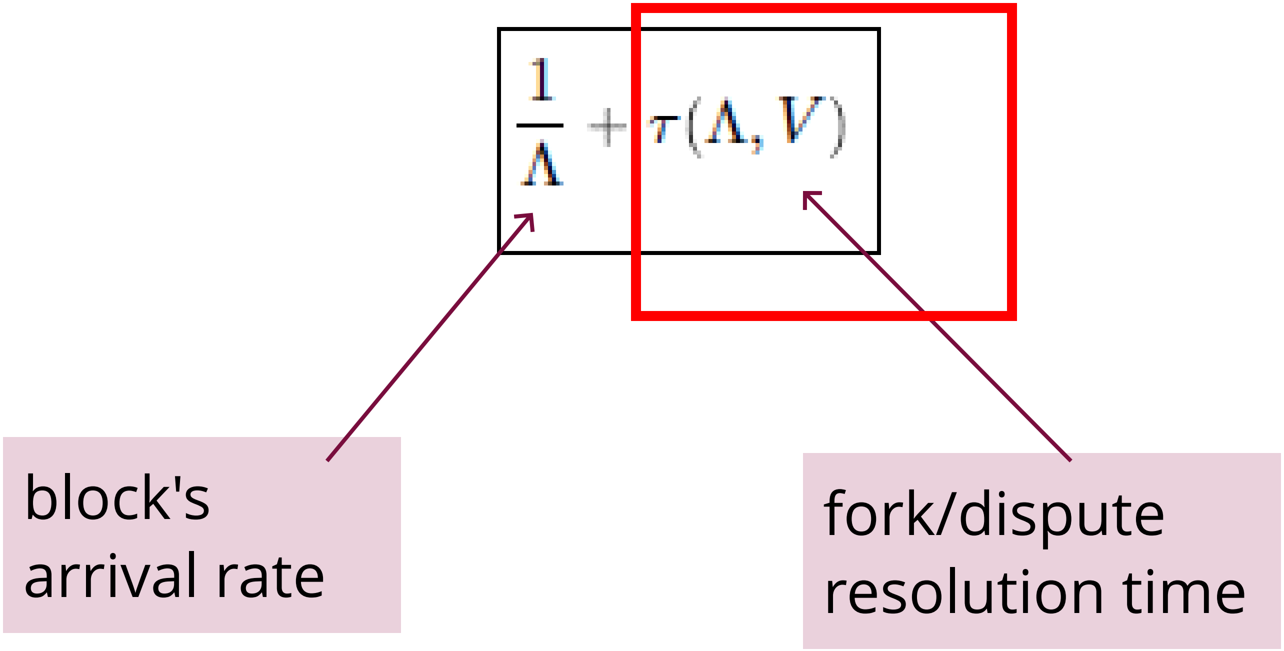
$$\boxed{\underbrace{\frac{1}{\Lambda}}_{\text{block's arrival rate}} + \underbrace{\tau(\Lambda, V)}_{\text{fork/dispute resolution time}}}$$

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:



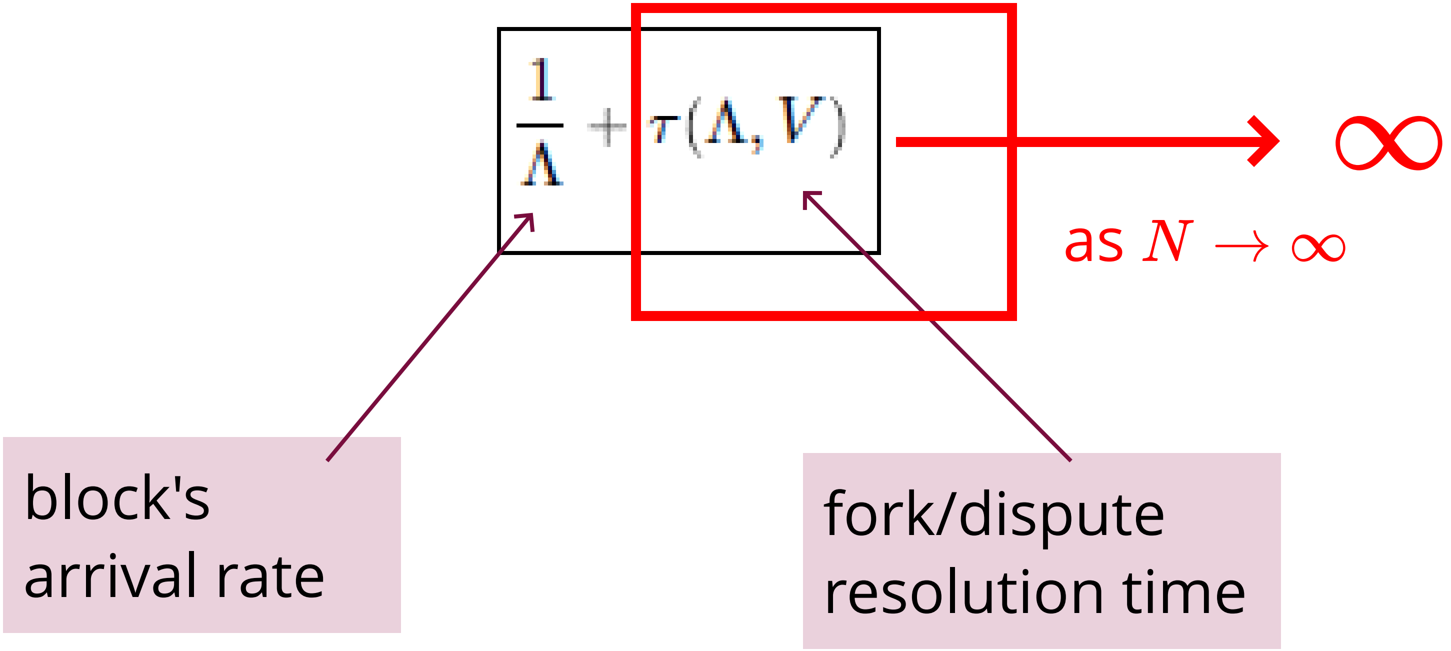
$$\boxed{\frac{1}{\Lambda} + \tau(\Lambda, V)}$$

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:



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

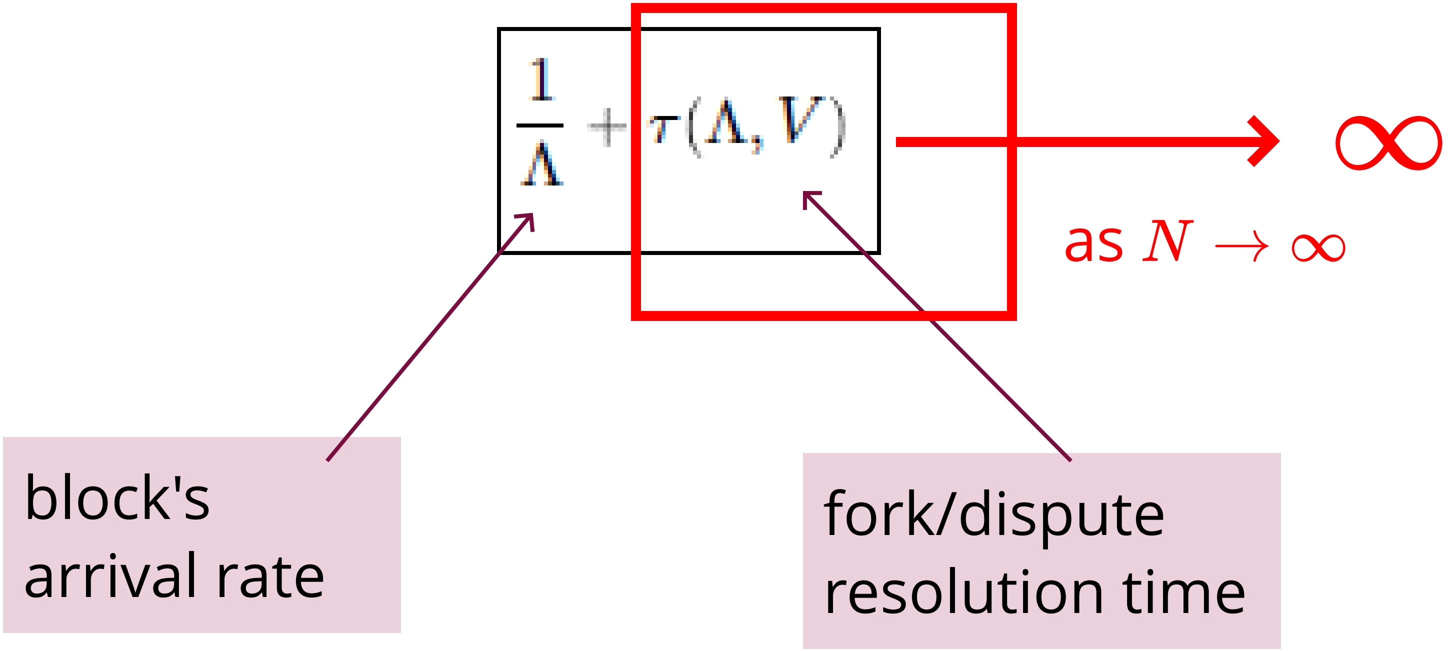
as $N \to \infty$

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:



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

as $N \rightarrow \infty$

block's arrival rate

fork/dispute resolution time

$c^* \rightarrow 0$

"limited adoption"

Comments/Questions:

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

Comments/Questions:

- Why do forks take ∞ to resolve?

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

Comments/Questions:

- Why do forks take ∞ to resolve?

Key Result:

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

Comments/Questions:

- Why do forks take ∞ to resolve?

Key Result:

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

Network delay/physical system limits

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

Comments/Questions:

- Why do forks take ∞ to resolve?

Key Result:

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

Lemma B.1 in Appendix B ....

Network delay/physical system limits

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

Comments/Questions:

Comments/Questions:

Number of validators V determined by free entry:

Comments/Questions:

Number of validators V determined by free entry:

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

Comments/Questions:

Number of validators V determined by free entry:

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

Comments/Questions:

Number of validators V determined by free entry:

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

Number of users $N \to \infty$

- $\Rightarrow$ expected fees $\to \infty$

Comments/Questions:

Number of validators V determined by free entry:

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

Number of users $N \to \infty$

- $\Rightarrow$ expected fees $\to \infty$

Comment 1: need more intuition for this:

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

Comments/Questions:

Number of validators V determined by free entry:

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

Number of users $N \to \infty$

- $\Rightarrow$ expected fees $\to \infty$

Comments/Questions:

Number of validators V determined by free entry:

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

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

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?

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?

Suggestion: better connections to existing literature

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.:
  - comp sci: Gilbert and Lynch (2002)
  - econ&finance: Abadi and Brunermeier (2018)
  - see Chen, Cong, Xiao (2019) for a survey

Suggestion: better connections to existing literature

- 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

@katyamalinova

malinovk@mcmaster.ca

slides.com/kmalinova

https://sites.google.com/site/katyamalinova/