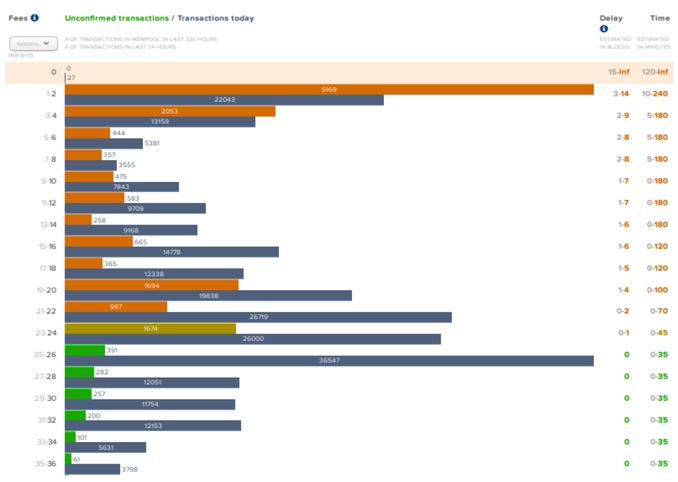
No Transaction Fees? No Problem! Achieving Fairness in Transaction Fee Mechanism Design

Sankarshan Damle, Varul Srivastava, and Sujit Gujar
Machine Learning Lab, IIIT, Hyderabad
sankarshan.damle@research.iiit.ac.in; varul.srivastava@research.iiit.ac.in; sujit.gujar@iiit.ac.in

AAMAS 2024 AUCKLAND NZ

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY HYDERABAD

Paper



- Transaction fees in Bitcoin were envisioned to be 'optional'
- In practice, transactions with marginal fee fail to get confirmed
- E.g., Users paying less fees have a waiting time of ≥ 9 blocks, while it is ≥ 14 blocks for those who pay an insignificant amount [4]

Bitcoin's Unfinished Business: Why Micropayments Still Matter

Tiny, cheap-to-deliver payments can open new markets for small digital goods. Can a new wave of crypto-inflected startups plug a longstanding gap in the internet? This piece is part of CoinDesk's Payments Week.

By David Z. Morris · Apr 29, 2022 at 12:15 a.m. · Updated Sep 19, 2023 at 9:33 p.m. · Layer 2

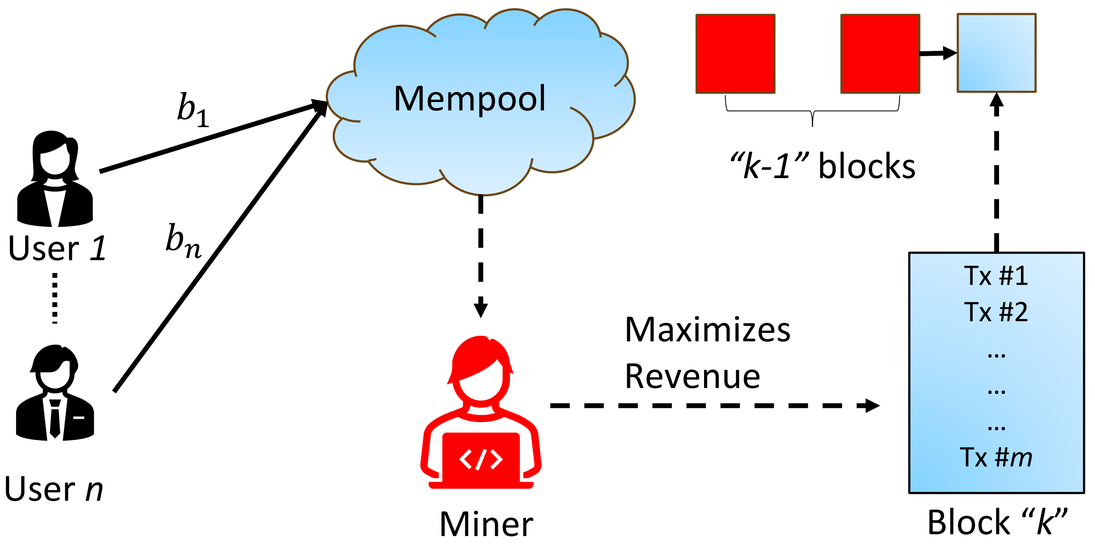
Credit: Coindesk

TECHNOLOGY

India's UPI Hits Record Volume

NOVEMBER 2, 2023

Credit: Global Finance



Transaction Fee Mechanisms (TFMs) [1]

Popular TFMs

- First-price Auction (FPA)
- Second-price Auction (SPA
- EIP-1559

Incentive Properties

- User Incentive Compatibility (UIC)
- Miner Incentive Compatibility (MIC)
- Off-chain Collusion Properties

Goal: To design TFMs that are fairer to the transaction creators (or users), while simultaneously preserving the incentive compatibility for both the miner and the users.

Fairness Notions for Transaction Fee Mechanisms

1) Zero-fee Transaction Inclusion (ZTi)
The probability with which a transaction t with transaction fee $b_t = 0$ gets included in a block B_k is strictly non-zero. That is, $\Pr(t \in B_k) > 0$.

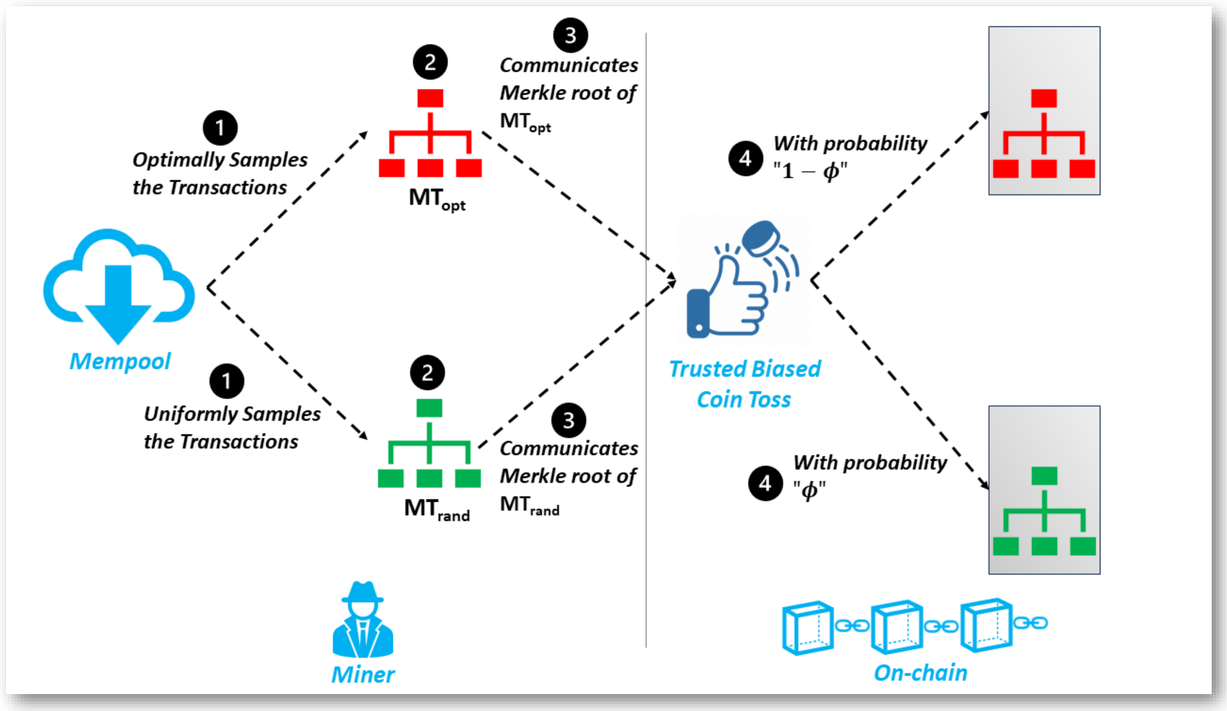
2) Monotonicity
The probability with which a transaction t gets included in a block B_k increases with an increase in its transaction fee b_t, given the remaining bids $\boldsymbol{b_{-t}}$ are fixed. That is, $\Pr(t \in B_k | \boldsymbol{b_{-t}}, b_t + \epsilon) > \Pr(t \in B_k | \boldsymbol{b_{-t}}, b_t)$ for any $\epsilon > 0$ and fixed $\boldsymbol{b_{-t}}$.

A TFM satisfying both our fairness notions ensures that each transaction has a non-zero probability of getting accepted!

Impossibility of Simultaneously Maximizing Miner Utility and Satisfying ZTi

Theorem (Informal). No TFM with a non-trivial payment rule, which provides a strategic miner complete control over the transactions to add to its block, satisfies Zero-fee Transaction Inclusion (ZTi).

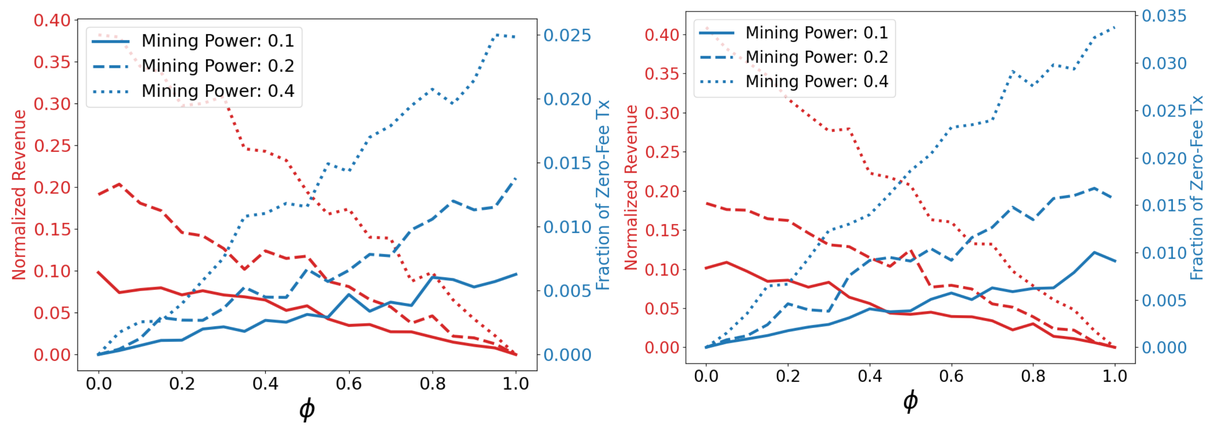
rTFM: Fairness in TFMs using On-chain Randomization



Trusted Biased Coin Toss:

$$O\big(Hash(B_k, \phi)\big) = Hash(B_k) < \phi \cdot TD \; ? \; \mathrm{MT_{rand}} : \mathrm{MT_{opt}}$$

rTFM: Empirical Evaluation



Uniform Bid Distribution | **Exponential Bid Distribution**

Results Summary:

We note that most existing TFMs do not satisfy ZTi. In contrast, rTFM – with an appropriate payment and burning rule – simultaneously satisfies our fairness notions along with UIC and MIC.

★Only if the base fee is "excessively low"

TFM	UIC	MIC	ZTi	Monotonicity
FPA [1]	✗	✓	✗	✓
SPA [1]	✓	✗	✗	✓
EIP-1559 [1]	✓★	✓	✗	✓
BitcoinZF [4]	✓	✗	✓	✓
rTFM + FPA	✗	✓	✓	✓
rTFM + FPA	✓★	✓	✓	✓

Key References

1. Roughgarden (2021). Transaction Fee Mechanism Design. In: EC
2. Chung and Shi (2023). Foundations of transaction fee mechanism design. In: SODA
3. Siddiqui et al. (2020). BitcoinF: Achieving Fairness for Bitcoin in Transaction-Fee-Only Model. In: AAMAS

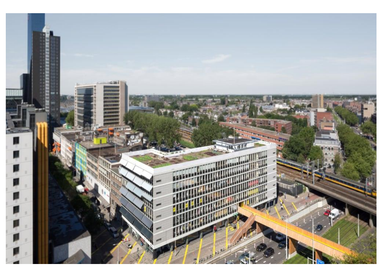
Analyzing Crowdfunding of Public Projects Under Dynamic Beliefs

Sankarshan Damle and Sujit Gujar
Machine Learning Lab, IIIT, Hyderabad
sankarshan.damle@research.iiit.ac.in; sujit.gujar@iiit.ac.in

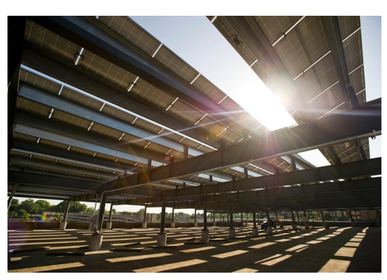
Paper

Crowdfunding of Public Projects

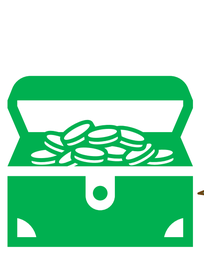
Crowdfunding is the process of raising voluntary funds, from a set of interested agents. Particularly, we focus on crowdfunding for public projects. E.g., public parks, libraries, bridges, and community services.



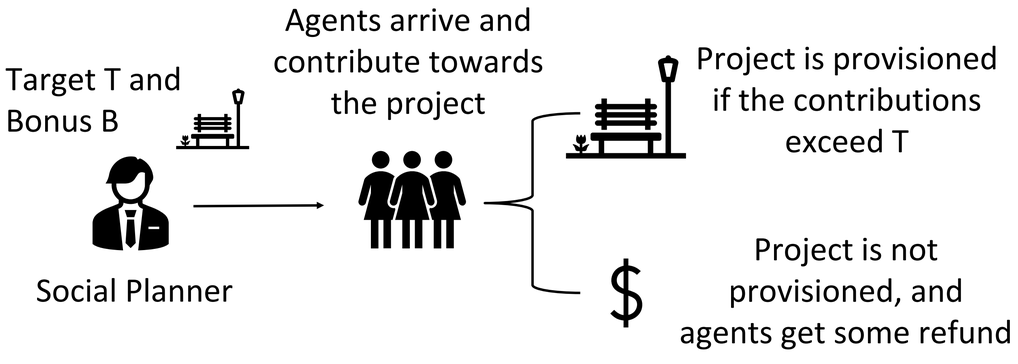
Wooden Pedestrian Bridge in Rotterdam



Solar Panels Installation in Memphis



Incentives help overcome the free-riding challenge and existence of inefficient equilibria!



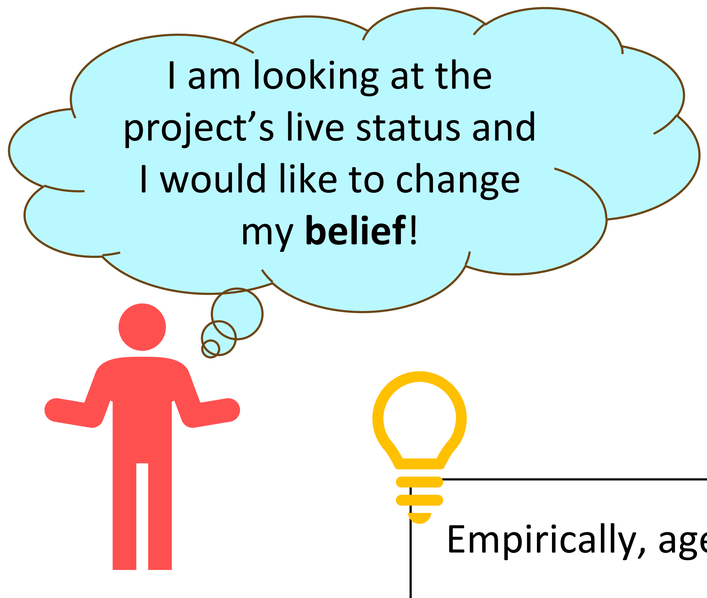
Provision Point Mechanism with Refunds (PPR) [1]

Non-efficient Equilibria

Seminal approaches for crowdfunding suffer from the existence of **inefficient** equilibria!

Free-riding Challenge

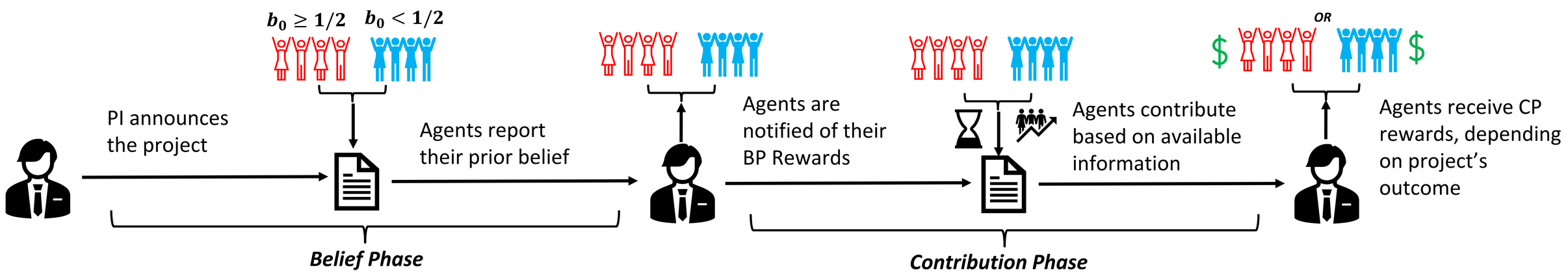
As public projects are **non-excludable**, strategic agents may prefer to **not** contribute towards the project's funding; instead, enjoy its benefits post crowdfunding!



Empirically, the probability of funding a project decreases with an increase in its duration

Empirically, agents prefer to contribute even in the absence of refunds

PPRx-DB: Crowdfunding of Public Projects under Dynamic Beliefs



Belief Phase (BP) Reward

- If $b_0 \geq 1/2$

$$\text{BP} := \frac{w}{\sum_{\{j \in A_H\}} w_j} \cdot B_B$$

- If $b_0 < 1/2$

$$\text{BP} := \frac{w}{\sum_{\{j \in A_L\}} w_j} \cdot B_B$$

Where, w is calculated using RBTS [4]

Contribution Phase (CP) Reward

- If the project is not funded

$$\text{CP} := \frac{x}{C_0} \cdot B_C$$

Where, C_0 is the total contribution to the project

Agent Utility Model

- If $b_0 \geq 1/2$

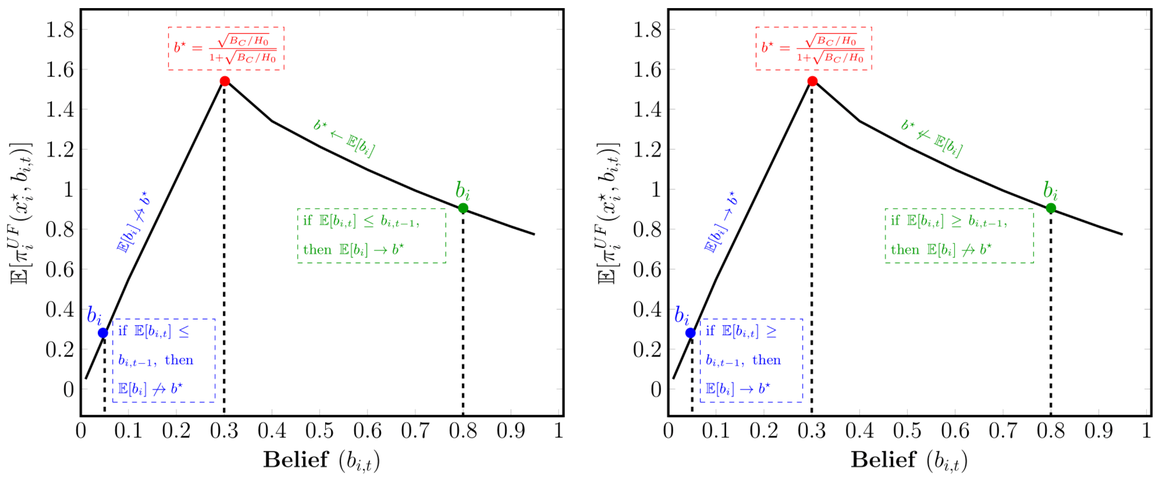
$$\text{Utility} := \mathrm{I}_{C_0 \geq H_0} \cdot (\theta - x + \text{BP}) + I_{C_0 < H_0} \cdot \text{CP}$$

- If $b_0 < 1/2$

$$\text{Utility} := \mathrm{I}_{C_0 \geq H_0} \cdot (\theta - x) + I_{C_0 < H_0} \cdot (\text{CP} + \text{BP})$$

Agent *i*'s Prior Belief	Agent Belief Update	Equilibrium Contribution	Equilibrium Time of Contribution	Race Condition
$b_{i,0} \geq 1/2$	Martingale	Closed-form	Deadline	Yes
	Super-martingale		At Arrival★	Yes/No★
	Sub-martingale		At Arrival★	Yes/No★
$b_{i,0} < 1/2$	Martingale	Closed-form	Deadline	Yes
	Super-martingale		At Arrival	No
	Sub-martingale		Deadline	Yes

★Depends on agent's prior belief and the random walks type



Proof for Deriving Equilibrium Time of Contribution when the Belief evolution is a Super-Martingale

Key References

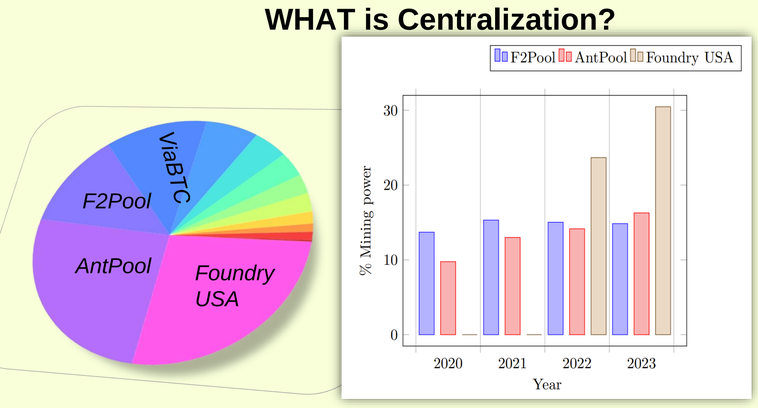
1. Zubrickas (2014). The provision point mechanism with refund bonuses. In: **Journal of Public Economics**
2. Damle et al. (2019). Civic Crowdfunding for Agents with Negative Valuations and Agents with Asymmetric Beliefs. In: **IJCAI**
3. Damle et al. (2023). Combinatorial Civic Crowdfunding with Budgeted Agents: Welfare Optimality at Equilibrium and Optimal Deviation. In: **AAAI**
4. Witkowski and Parkes (2012). A Robust Bayesian Truth Serum for Small Populations. In: **AAAI**

DecentBRM: Decentralization through Block Reward Mechanisms

Varul Srivastava and Sujit Gujar
Machine Learning Lab, IIIT, Hyderabad
varul.srivastava@research.iiit.ac.in sujit.gujar@iiit.ac.in

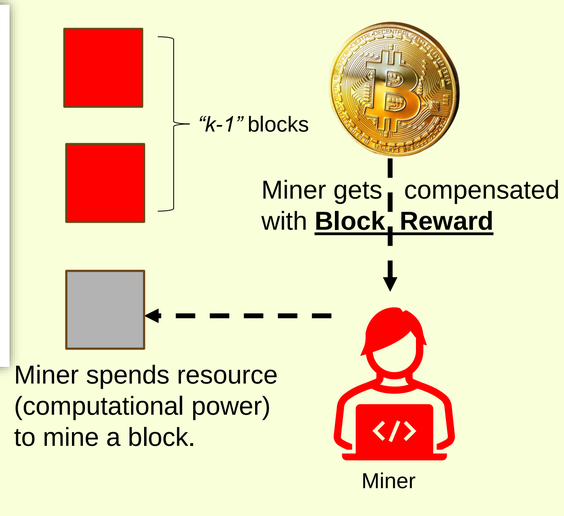
Question: Are Proof-of-Work (PoW) Blockchains truly decentralized?

WHAT is Centralization?



Solo Mining: Get 1 Bitcoin 1/100 times.
Join Mining Pool: Get 0.1 Bitcoin 1/10 times.

WHY does it happen?



PoW mining

What would you rather pick $100 bill or a lottery ticket?

Choice 1: Get $1 million with a probability of 1/10,000
Choice 2: Get $100 with certainty.

*Both choices have same expected reward, but **Choice 2** is preferred by many as has lesser variance.*

Takeaway: Out of different strategies with same expected payoff, **risk-averse** players opt for a lower variance strategy.

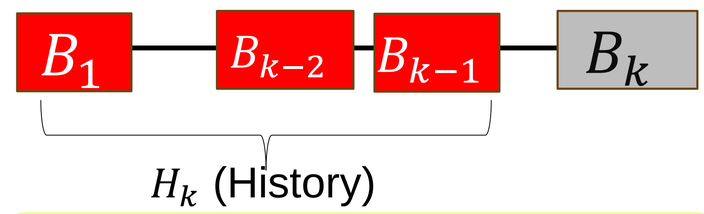
HOW does it impact blockchain?

Centralized Bitcoin → Insecure Bitcoin

PoW blockchain security relies on honest majority. Mining pools pose a threat to this through "centralization of power"

Block Reward Mechanisms (BRM)

Definition: BRMs are mechanisms to distribute cryptocurrency (payment) among miners for participating in the (cost consuming) mining process.

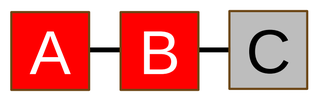


$$\text{BRM} = \Gamma(H_k, B_k)$$

- Memoryless BRM $\Gamma(H^1{}_k, B_k) = \Gamma(H^2{}_k, B_k)$
- Retentive BRM $\Gamma(H^1{}_k, B_k) \neq \Gamma(H^2{}_k, B_k)$

Rewards for a block are *independent of history* of the blockchain ledger.

Memoryless BRMs

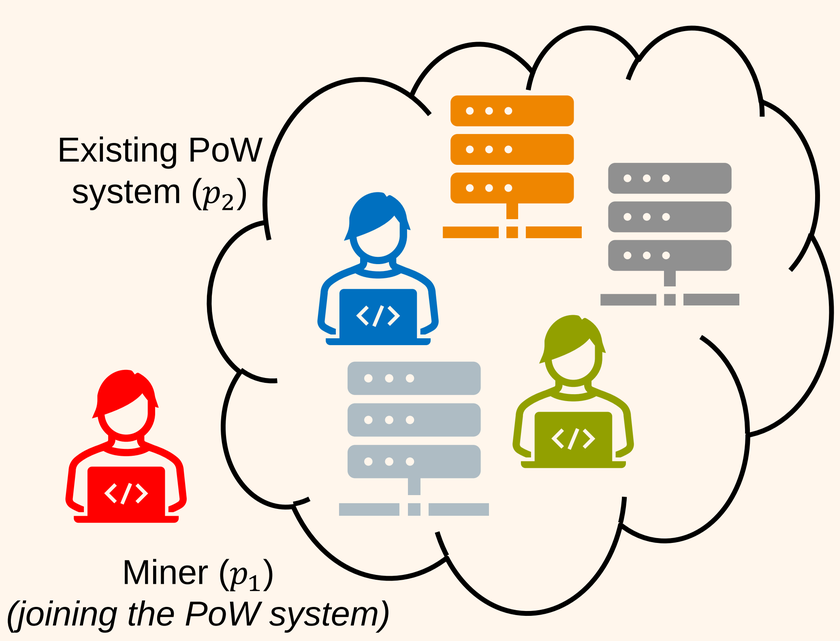


Rewards for a block is *dependent of history* of the blockchain ledger.

Retentive BRMs

Reward for block C in both chains is same in Memoryless BRMs and (can be) different for Retentive BRMs.

Modelling as a Game/Optimization Problem



Players:
p_1 is the *miner joining the system*.
p_1 has mining power $\boldsymbol{M_1}$ and risk averseness $\boldsymbol{\rho}$

p_2 is the *current PoW system*.
p_2 has mining power $\boldsymbol{M_2}$ $\quad (M_2 \gg M_1)$

There are $\boldsymbol{n}$ mining pools, each controlling $\boldsymbol{f_i}$ fraction of M_2

Strategy Space:
Strategy for p_1 is choosing
$$\boldsymbol{g} := \{g_0, g_1, g_2, \dots, g_n\}$$
g_i is fraction of M_1 given to pool i

Strategy for p_2 is choosing
$$\boldsymbol{f} := \{f_1, f_2, \dots, f_n\}$$

Game Progression: (Stackelberg type game)
1. $\boldsymbol{p_2}$ chooses $\boldsymbol{f}$
2. $\boldsymbol{p_1}$ chooses $\boldsymbol{g}$ with the knowledge of $\boldsymbol{f}$

Reward: Each block is mined by pool i with probability $z_i := \frac{f_i M_2 + g_i M_1}{M_1 + M_2}$. Reward for round k:
$$R_k = \Gamma(H_k, B_k)\psi_i \qquad w.p.\ z_i$$

Utility: Utility is given for p_1 with (M_1, ρ) is:
$$U = \underbrace{a\boldsymbol{E}[\boldsymbol{R_k}]}_{\text{Expected Reward}} + \underbrace{b\left(\boldsymbol{E}\left[\boldsymbol{R_k^\rho}\right]\right)^{\boldsymbol{1/\rho}}}_{\text{RISK}} - \underbrace{c\ D(\boldsymbol{g})}_{\text{Switching Cost (Penalty)}}$$

Decentralization: A PoW blockchain is decentralized if the following holds:
$$\arg\max_i f_i \geq \arg\max_i \frac{f_i M_1 + g_i M_2}{M_1 + M_2}$$

Theoretical Results

For *Memoryless BRMs*

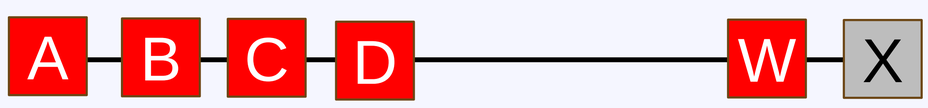
Theorem (Informal). It is impossible to have a decentralized PoW system using a *Memoryless Reward Mechanism* when $c \geq \underline{c}$.

For *Retentive BRMs*

For Retentive BRMs:
- Risk is reduced (still non-zero).
- Fruitchain[1] is still centralized (pool formation incentivized)

DecentBRM[2]

DecentBRM *A Retentive BRM* which has higher utility for solo mining than pool formation.



Block Reward Rule: For any new block X, total reward R_{block} for block X is distributed equally among all miners till block X equally.

Theorem (Informal). Following solo-mining in DecentBRM is (weakly dominant) equilibrium strategy for p_1 after T rounds of the protocol.

DecentBRM serves as existence proof for decentralized Retentive BRMs.

[1]Rafael Pass and Elaine Shi. 2017. FruitChains: A Fair Blockchain. In Proceedings of the ACM Symposium on Principles of Distributed Computing (PODC '17).

[2]Srivastava, Varul, and Sujit Gujar. "DECENT-BRM: Decentralization through Block Reward Mechanisms." *arXiv preprint arXiv:2401.08988* (2024).