Impossibility of Decentralized Trading on Permissionless Blockchains

Hanna Halaburda
NYU Stern

CAAW

March 6, 2026

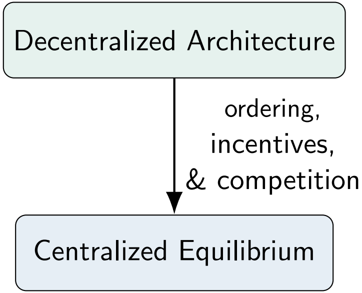
Blockchain Architecture vs. Equilibrium

Architecture (Design Goals)

- Transparent
- Decentralized (permissionless)
- Fair and verifiable

Equilibrium (Observed)

- Opaque power structures re-emerge
- Concentration of block creation
- Rent extraction from trading (MEV)



Decentralized Architecture

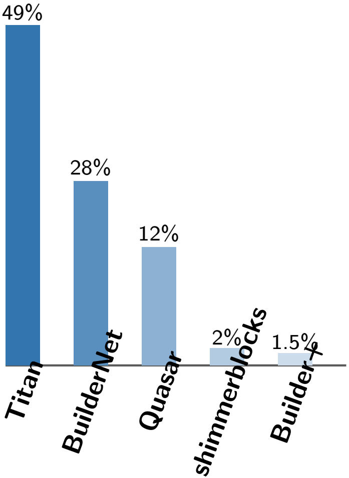
ordering,
incentives,
& competition

Centralized Equilibrium

the architecture can be decentralized
while the economic equilibrium becomes centralized

Concentration in Practice

- A small set of block builders capture the vast majority of blocks
- MEV extraction is economically meaningful (hundreds of millions USD)
- Private order-flow channels intermediate most transactions



Top builder market shares
Ethereum (30-day window, Dec 2025)
Source: *Rated Network* (www.rated.nework)

… despite Ethereum Following the Canonical Decentralization Playbook

Each major Ethereum design choice was motivated by standard decentralization logic:

- **Permissionless entry** → prevent gatekeeping and exclusion
- **Public mempool / transparency** → fairness, auditability, neutral access
- **Proof-of-Stake** → reduce hardware-driven scale economies
- **Proposer–Builder Separation (PBS)** → separate roles, increase competition, reduce MEV abuse

concentration intensifies after decentralization updates

What has been already shown

What we already know

- MEV exists and is economically meaningful
  (Daian et al. 2019; Milionis et al. 2024; Heimbach, Pahari & Schertenleib 2024)
- Block building is highly concentrated
  (Heimbach et al. 2023; Wahrstätter et al. 2023)
- Exclusive orderflow dominates outcomes
  (Pahari & Canidio 2025; Oz et al. 2024; Thiery 2023)
- Winners are persistent and builder-specific
  (Canidio & Pahari 2025; Wu et al. 2025)
- Contest-based block construction can centralize under PBS
  (Gupta, Pai & Resnick 2023; Capponi, Jia & Olafsson 2024)

What is not yet explained

- Whether decentralized routing can survive in equilibrium
- Whether dominance depends on the protocol design
- Why removing frictions to competition produces more concentration

removing frictions does not level the playing field — it steepens it

Starting with Permissionless Blockchain Basics (with DeFi capability)

user tx → public mempool (or not) → block creator → block

- One block at a time
- Ordering / selecting / inserting transactions affects payoffs (MEV)
- Open contestable competition over ordering
- Symmetric rules and entry by design

open competition over transaction ordering does not discipline concentration — it generates it

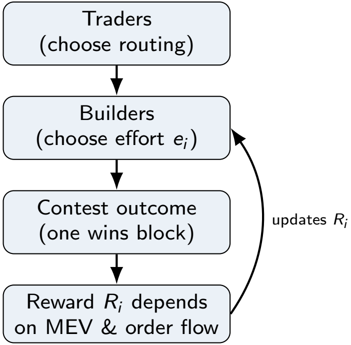
Modeling Incentives

- potential **block creators** (eg, builders, validators, miners)
    - each chooses effort $e_i \geq 0$ to compete for the next block (mining, staking, auction)
    - success probability (Tullock contest):

$$p_i(\mathbf{e}) = \frac{e_i^a}{\sum_k e_k^a}, \qquad a \geq 1$$

    - payoff: $\Pi_i(\mathbf{e}; R_i) = p_i(\mathbf{e})\, R_i - \text{costs}(e_i)$
    - reward R_i reflects both protocol reward and value extracted from trades:

$$R_i = R + r_i\, B_i, \quad B_i = \text{trading volume handled (public + private)}$$



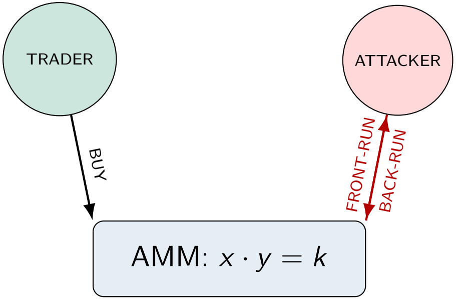
- **traders** choose where to route their transaction:

private flow to builder j: $U_{\text{priv}}(j) = p_j(1-r_j)\, v$ or public mempool: $U_{\text{pub}} = (1-\tau_M)\, v$,

Mechanism 1: Payoff-Relevant Ordering → Extractable Rent

Sandwich (AMM) in 4 steps

1. Trader posts buy; order becomes observable
2. Attacker front-runs (buys) ⇒ pushes price up
3. Trader executes at worse price
4. Attacker back-runs (sells) ⇒ captures spread



Payoff-relevant ordering ⇒ extractable rents (MEV)

- Ordering, selecting or inserting transactions create extractable rents (MEV)
- Block creators differ in extraction ability
- Same rules, different realized payoffs (R_i)

Transparency is not required but widens dispersion. Transparency equalizes information — not the ability to profit from it

more of the model: contest for right to create a new block

success probability (Tullock contest with decisiveness $a \geq 1$):

$$p(\mathbf{e}) = \frac{e_i^{a}}{\sum_{k=1}^{N} e_k^{a}}, \qquad \lim_{a\to\infty} p = \begin{cases} 1/|\arg\max_k e_k| & \text{for ties on } e_{\max}, \\ 0 & \text{otherwise.} \end{cases}$$

cost & payoff:

$$C(\mathbf{e}) = \alpha(e_i) + \beta(e_i)\,p(\mathbf{e}) + \gamma(e_{-i})\,p(\mathbf{e}), \qquad \Pi_i = p(\mathbf{e})\left[R_i - \beta(e_i) - \gamma(e_{-i})\right] - \alpha(e_i)$$

- α, β – continuous, non-decreasing, weakly convex
- γ – continuous, non-decreasing label-neutral aggregator of others' effort ($\max_{k\neq i} e_k$, sum, etc)

mappings to canonical environments:

- PoW/PoS: $a = 1$, $\alpha(e_i) = c\,e_i$, $\beta \equiv 0$, $\gamma \equiv 0$
- All-pay, winner-take-all: $a \to \infty$, $\alpha(e_i) = e_i$, $\beta \equiv 0$, $\gamma \equiv 0$
- First-price, winner-take-all: $a \to \infty$, $\alpha \equiv 0$, $\beta(e_i) = e_i$, $\gamma \equiv 0$
- Second-price, winner-take-all: $a \to \infty$, $\alpha \equiv 0$, $\beta \equiv 0$, $\gamma(e_{-i}) = \max_{k\neq i} e_k$

Mechanism 2: Competition Sorts and Amplifies Differences

- Each round one block is created; winner receives reward
- Agents exert effort; probability of winning rises with effort share
- Contests differ in decisiveness: from diffuse (PoW-like) to auctions (PBS-like)

Theorem (Sorting)

higher reward $R_i \Rightarrow$ higher optimal effort $e_i^* \Rightarrow$ higher winning probability p_i^*.
(holds also for mixed strategies, and random reward)

Proposition (Decisiveness $\uparrow \Rightarrow$ Concentration $\uparrow$)

As contest becomes more decisive ($a \uparrow$), same differences in R_i translate into larger differences in p_i^*

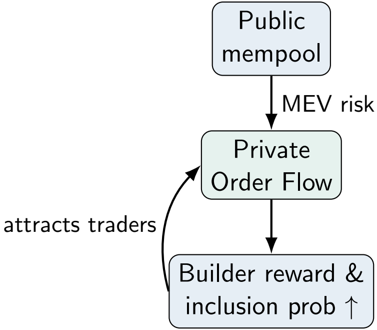
Ethereum:

- Increasingly clean and decisive contests (PoW → PoS → PBS)
- Small differences become large outcome gaps

competition does not just allocate outcomes – it amplifies heterogeneity

Mechanism 3: Trader response makes it worse

- Public mempool → extraction risk, $U_{\text{pub}} = (1 - \tau_M)\, v$
- Traders route privately to a builder, $U_{\text{priv}}(j) = p_j(1 - r_j)\, v$
- Preference for builder with higher inclusion probability (p_i^*)
- Builder with more private order flow (POF) gets higher reward $(R_i) \Rightarrow$ higher inclusion probability

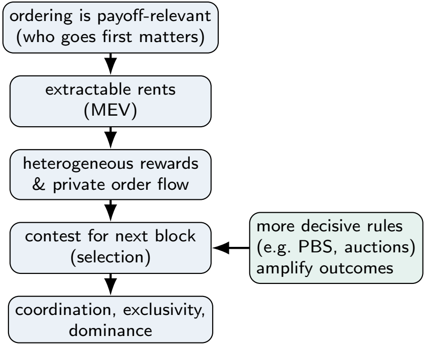


routing creates coordination externalities around execution reliability:
more POF $\Rightarrow R_i \uparrow \Rightarrow p_i^* \uparrow \Rightarrow$ **more POF**

market sharing is unstable, and
monopoly is stable when traders choose builders

Putting It Together: Why Blockchain Markets Centralize

1. **Payoff-relevant ordering**
   Who goes first affects payoffs ⇒ extractable rents (MEV) ⇒ heterogeneous rewards
2. **Decisive contests**
   Competition for the next block sorts agents and amplifies small reward differences
3. **Private routing**
   Traders respond by routing privately ⇒ coordination and exclusivity; sharing is unstable


ordering is payoff-relevant (who goes first matters)
extractable rents (MEV)
heterogeneous rewards & private order flow
contest for next block (selection)
more decisive rules (e.g. PBS, auctions) amplify outcomes
coordination, exclusivity, dominance

Why Ethereum's decentralization updates backfired

- **Transparency** makes payoff-relevant opportunities predictable, widening reward dispersion
- **PoS** made POF more appealing
- **PBS / auctions** make contests more decisive, amplifying small differences
- **Specialization** (builders, relays) sharpens heterogeneity in extraction ability

architecture decentralizes access – equilibrium centralizes control

This Is Not a Blockchain Anomaly

- **Ordering affects payoffs:** being earlier or selected creates surplus
- **Open competition over ordering:** many agents compete for the right to decide who goes first
- **Heterogeneous gains from ordering:** some benefit more from controlling ordering than others

General result

When these conditions hold, competition over *who goes first* can generate **coordination, exclusivity, and persistent dominance** in equilibrium — even in the absence of network effects in utilities or scale economies in costs.

Transparency is not required — but makes the mechanism easier to observe and harder to avoid.

This Matters Beyond Crypto

- Ad auctions / ranking
  a small number of top-ranked ad or search-result slots capture most clicks and conversions
  Google (search ads) and Amazon (sponsored products)
- Cloud scheduling / compute queues
  high-end GPUs/TPUs are scarce
  AWS and Azure
- Matching with priority (jobs)
  matching or exposure; top placement and early consideration are limited
  LinedIn, Upwork/Fiverr

whenever ranking/priority is scarce and payoff-relevant, expect coordination and dominance to reappear, even without network effects in primitives

open architecture does not neutralize economic forces leading to centralization — it may even magnify them

Impossibility of Decentralized Trading on Permissionless Blockchains

Hanna Halaburda
NYU Stern

CAAW

March 6, 2026

Multihoming Does Not Rescue Decentralization

Trader behavior (given builders)

- Traders may route to $m > 1$ builders at cost $\ell(m)$
- They include the top m^* builders with highest surplus $S_i = p_i(1 - r_i)$ exceeding duplication cost

Builder behavior (given routing)

- Builders set fees r_i to maximize profit given incoming flow
- Any builder included by traders prices up to the participation cutoff
- Thus all included builders deliver the same surplus S_i

Market sharing is unstable when $\Delta\ell(2) > 0$

- A small reallocation of flow lowers the weaker builder's inclusion probability
- Its surplus falls below the duplication threshold ($S_i \leq p_i$, which declines as well)
- Traders strictly drop it (further decreasing p_i)

$\Longrightarrow$ market-sharing allocations unravel; the only robust equilibrium is monopoly private order flow

Market-sharing equilibria exist under costless multihoming admits (knife-edge)

Backup: formal arguments

Contest success (Tullock): $p_i(\mathbf{e}) = \frac{e_i^a}{\sum_k e_k^a}$ $(a \uparrow \Rightarrow$ more winner-take-all)

Block creator (builder / validator / miner)

$$u_i(\mathbf{e}; R_i) = p_i(\mathbf{e}) \left(R_i - \beta(e_i) - \gamma(S(\mathbf{e}))\right) \; - \; \alpha(e_i).$$

Sorting intuition: higher effective reward $R_i \Rightarrow$ higher optimal effort $e_i^* \Rightarrow$ larger p_i^*.

Two amplifiers of concentration:

- $a \uparrow$ magnifies odds ratios $\left(\frac{p_i}{p_j} = \left(\frac{e_i}{e_j}\right)^a\right)$
- Greater dispersion in R_i raises top shares

Trader

$$\Pi_{\text{public}} \;=\; v\,(1-\tau_M), \qquad \tau_M \;=\; \sum_i p_i\, r_i,$$

$$\Pi_{\text{POF}(j)} \;=\; p_j\, v\,(1-r_j), \qquad \text{route to } j \text{ with maximal } p_j(1-r_j) \text{ if } p_j(1-r_j) > 1-\tau_M.$$

POF stability sketch: Equal sharing unstable (profitable deviation to larger pool); monopoly stable (single deviation suffers lower inclusion probability).