Sybil-proof Mechanisms

The coolest theorem of 2024 and its implications for APS/PBS

Christoph Schlegel

Research, Flashbots

Can we have a decentralized builder market?

Motivation

- More precisely, suppose you
  - want to to allocate the right to propose blocks,
  - in a permission-less system (Sybils 😱),
  - and don’t want to always allocate the right to the same proposer.
- Is there **any mechanism** that would do that?

Motivation

- Value of proposing same to everyone (and known): Many solutions…
- In reality
  - value of proposing is different to different parties,
  - depends on private information.
  - That’s why there is a secondary market (aka MEV boost)...
  - Caveat: How much private value and info there is depends on market structure.
- With private value, we need to incentivize proposers to tell us their value.

Mechanism Design Approach

- What is the full design space of IC & Sybil-proof mechanisms?
- For IC, Myerson tells us to look into monotonic allocation rules e.g.
    - Allocate to the highest value bidder.
    - Run a lottery with equal chances for everyone.
    - Run a lottery with chances proportional to value.
    - Etc.
- Only one (symmetric) monotonic allocation rule gives a Sybil-proof mechanism!

Theorem

The only non-wasteful, symmetric, IC, Sybil-proof mechanism is a second price auction with symmetric tie breaking.

Any market structure with significant private value will lead to builder centralization.

Private Value and Market Structure

- Main reasons for private value:
  - private and exclusive order flow
  - Builder/Proposer-Searcher integration

- **Allocate the right in advance** to remove private value (PoS, execution tickets)?
- **Constrain the proposer** to remove private value (ILs, MCP)?

Allocate proposal rights in advance

- Allocate the right in advance to remove private value?
  - E.g. PoS, execution tickets/auctions

- **Secondary market**
- But upstream effect:
  - All private value is removed, bc all flow goes to the winning proposer (less likely)
  - Always have out of protocol secondary market (more likely)

Constrain the proposer

- **Inclusion Lists**
  - Doesn't remove builder centralization but deals with some of its negative effects
- **Deterministic Ordering** (e.g. priority ordering)
  - Could remove it, but has other trade-offs.
- **Multiple concurrent proposers**
  - With significant private value same result applies:

    one proposer secures all rights!
  - Is there a version of MCP without significant private value for proposers? TBD

Conclusion

- We can propose another dozen PBS/APS solutions
  - Claim: they will all lead to builder market centralization.
  - If we avoid some censorship through IL it's still a net improvement.

- Two potential ways out:
  - Modularizing & decentralizing the builder role
  - Constrain builder so much that they cannot extract significant information rent
    - Is there a good design for it?

Thank you!

Christoph Schlegel

Researcher, Flashbots

christoph@flashbots.net

https://arxiv.org/abs/2407.14485