The Tension Between MEV and Censorship Resistance

Julian Ma

Robust Incentives Group

Ethereum Foundation Research

Aligning Values

- MEV is the maximum private benefit the Extractor can achieve.
- Ethereum Protocol aims to maximize social benefit.
  - Censorship Resistance is one core value.
- The Extractor is an agent of the Protocol.

The ecosystem needs to align private benefit with social benefit.

Observations on Censorship

Economic Censorship

e.g. Liquidation Censorship

Accidental Censorship

e.g. Timing Games

Regulatory Censorship

e.g. Government Censorship

Observations on Censorship

Economic Censorship

e.g. Liquidation Censorship

Accidental Censorship

e.g. Timing Games

Regulatory Censorship

e.g. Government Censorship

Conclusion: Values are currently unaligned.

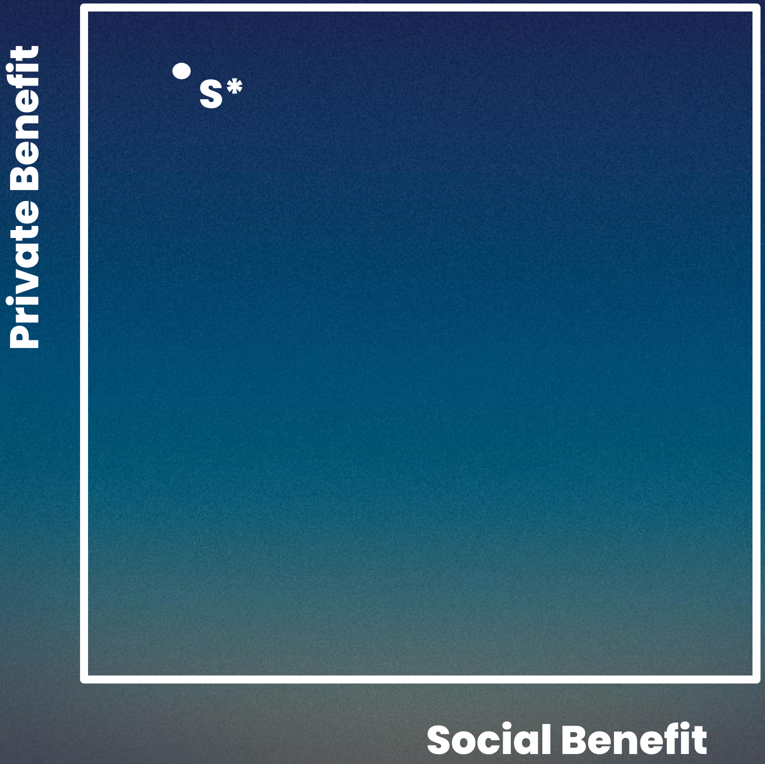
Section 1

Value Aligning Design Philosophy.

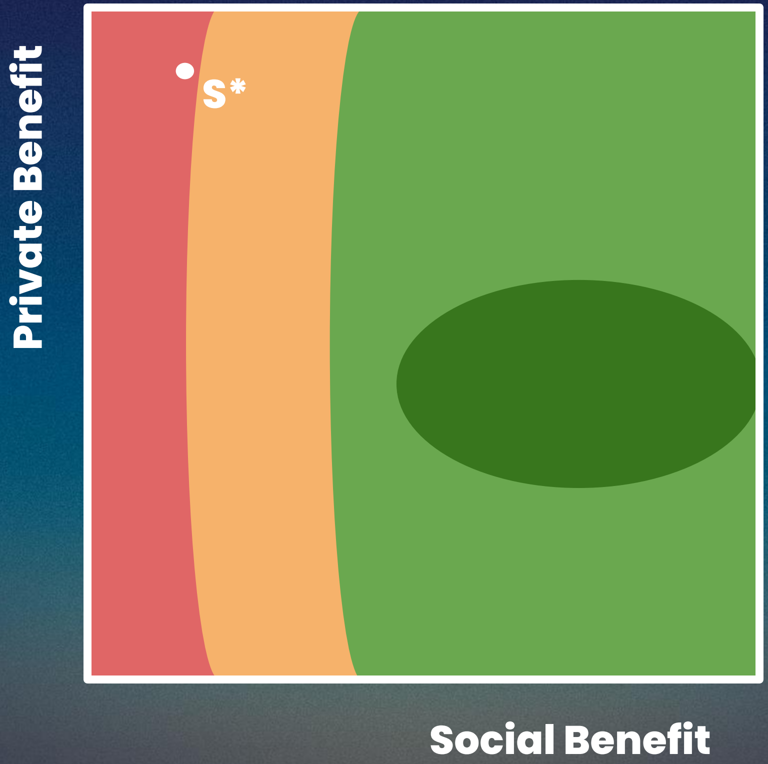
MEV is extracted via State Transition Function

$$\gamma(S,T) \rightarrow S'$$

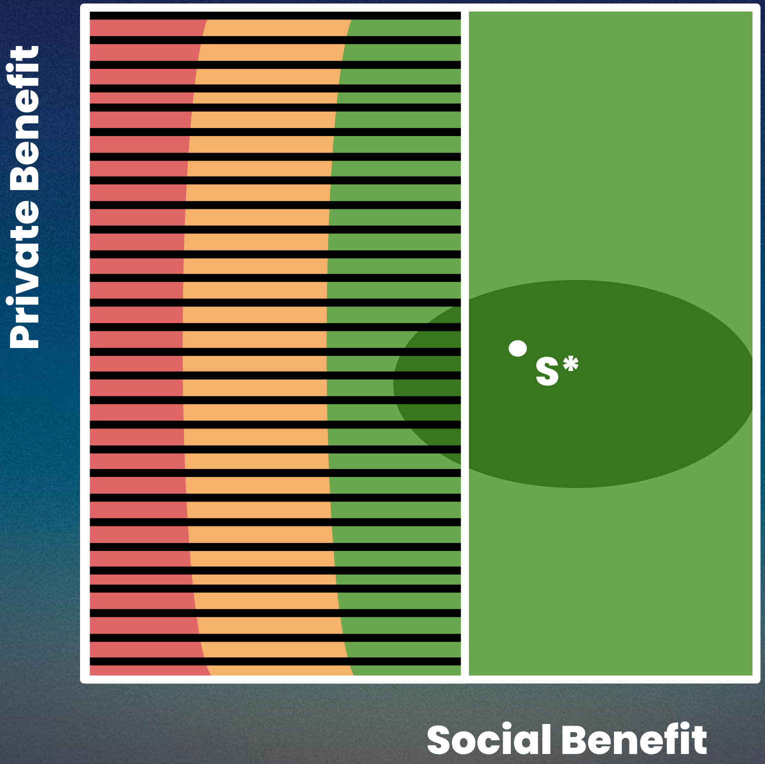
Mapping States to Private and Social Benefit



Granularity of Ethereum's Beliefs



Imposing Constraints

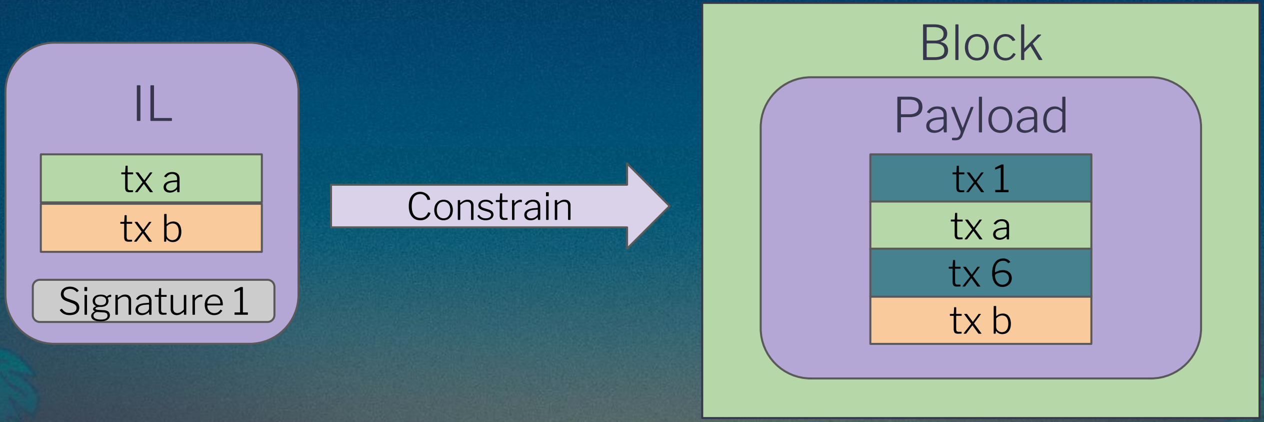


Section 2

Inclusion List Case Study.

Inclusion List Design Philosophy

- Allow the most decentralized participants to have some input into centralized block construction.
- No MEV can be extracted by the Inclusion List creator.
- Goal: Increase Chain Neutrality.

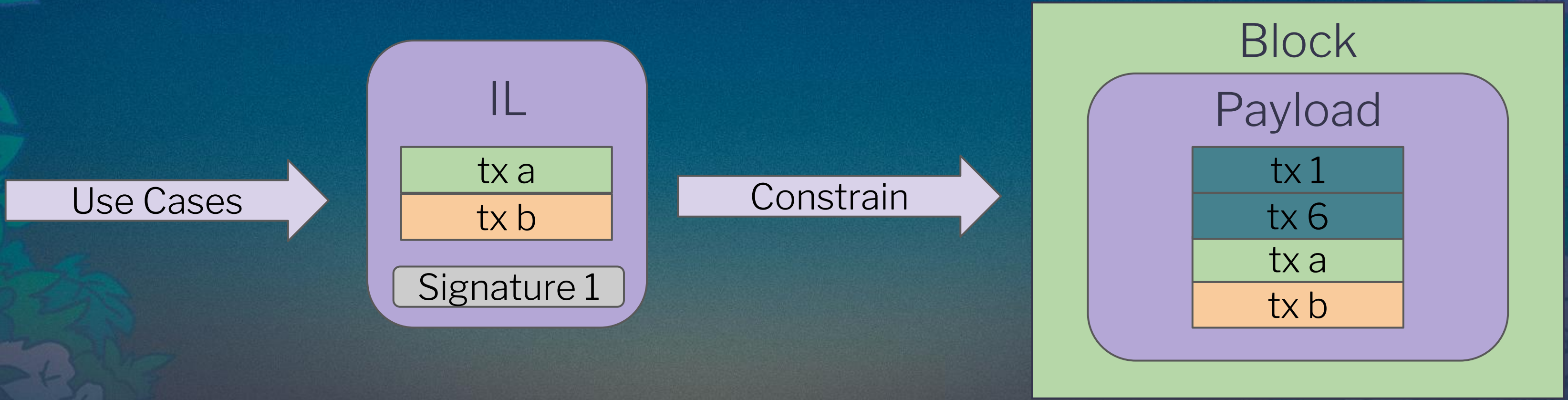


Uncrowdability

- **Informal Definition:** The inclusion list creates more value for the inclusion list creator if used as intended.
- No other use cases can crowd the inclusion list.
  - Preconfirmations.
  - MEV extraction.
- Inclusion list must be **minimally invasive** such that the intended constraint is achieved.
- Otherwise, private benefit of inclusion list creator may differ from social benefit.
  - If private benefits differ, it will lead to centralization.

Unconditional vs Conditional

- **Unconditional:** All inclusion list transactions must be included regardless of whether the block is full.
- If a transaction is in the unconditional inclusion list, it will be included on-chain.
    - Potentially more crowding out.

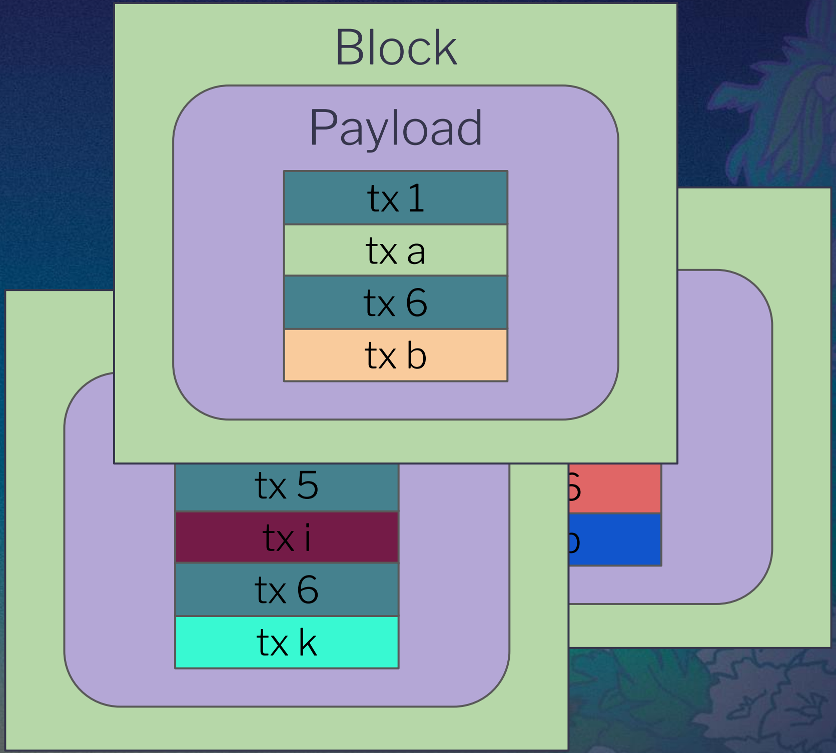


Section 3

Multiple Concurrent Block Producers Case Study

Basic Idea

- There are multiple block producers acting simultaneously.
- Goal: Prevent Economic Censorship.
  - Decrease expected **adverse selection.**
- **Mechanstein:** Top-of-block and Rest-of-block Payloads [Barnabé and Mike].
- **BRAID:** Deterministic merger of *k* chains [Max].

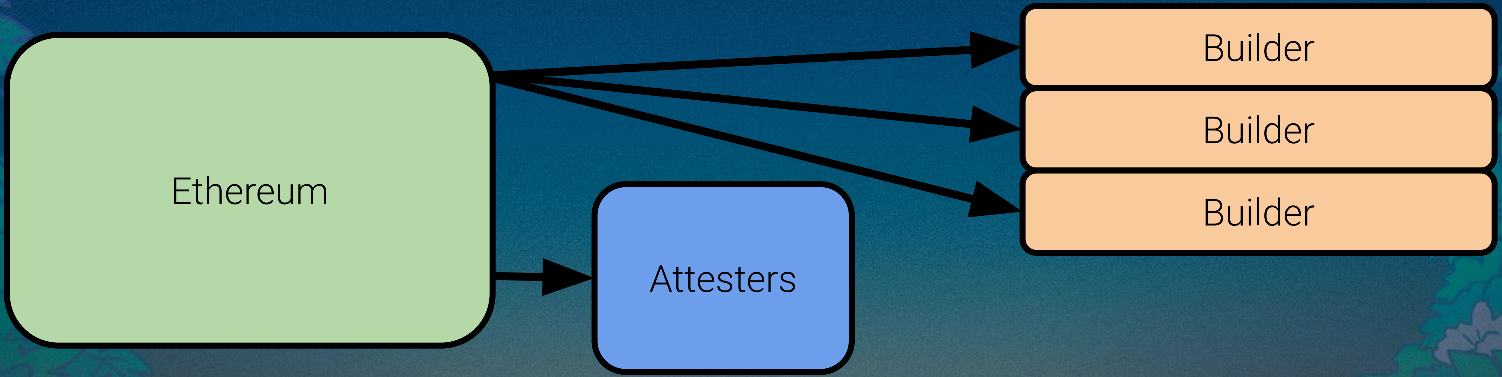


Uncrowdability Score

- MCBP specifically designed for the gain in censorship resistance for transactions where there may be adverse selection.
- **It allows any block producer to extract MEV equally well.**
- Partial block is a vehicle for MEV.
- Cannot expect a large set of participants to have competitive private valuations because of:
  - Returns to scale.
  - Return to sophistication.
  - Barriers to entry.

Dependency on Attester-Proposer Separation (APS)

- MCBP is Crowdable, so its creators will be fairly centralized.
- **Thus, need to ensure its creators are not also attesters!**
- **APS unlocks new block construction pipeline!**



Section 4

Consequences.

Applications Consuming Consensus Information

- Assume we have an ✨ **Uncrowdable** ✨ Inclusion List.
- It is unlikely it will contain arbitrage transactions.
- May treat transactions from the IL differently.
  - Example: Asymmetric Speedbump
  - Inclusion list transactions may take liquidity.
  - Other transactions may provide liquidity.
- **Seemingly:** I believe that you believe that I believe…

Applications Consuming Consensus Information

- Assume
- It is unli
- May tre
  - Ex
  - IL
  - Ot
- **Seemin**

Applications Consuming Consensus Information

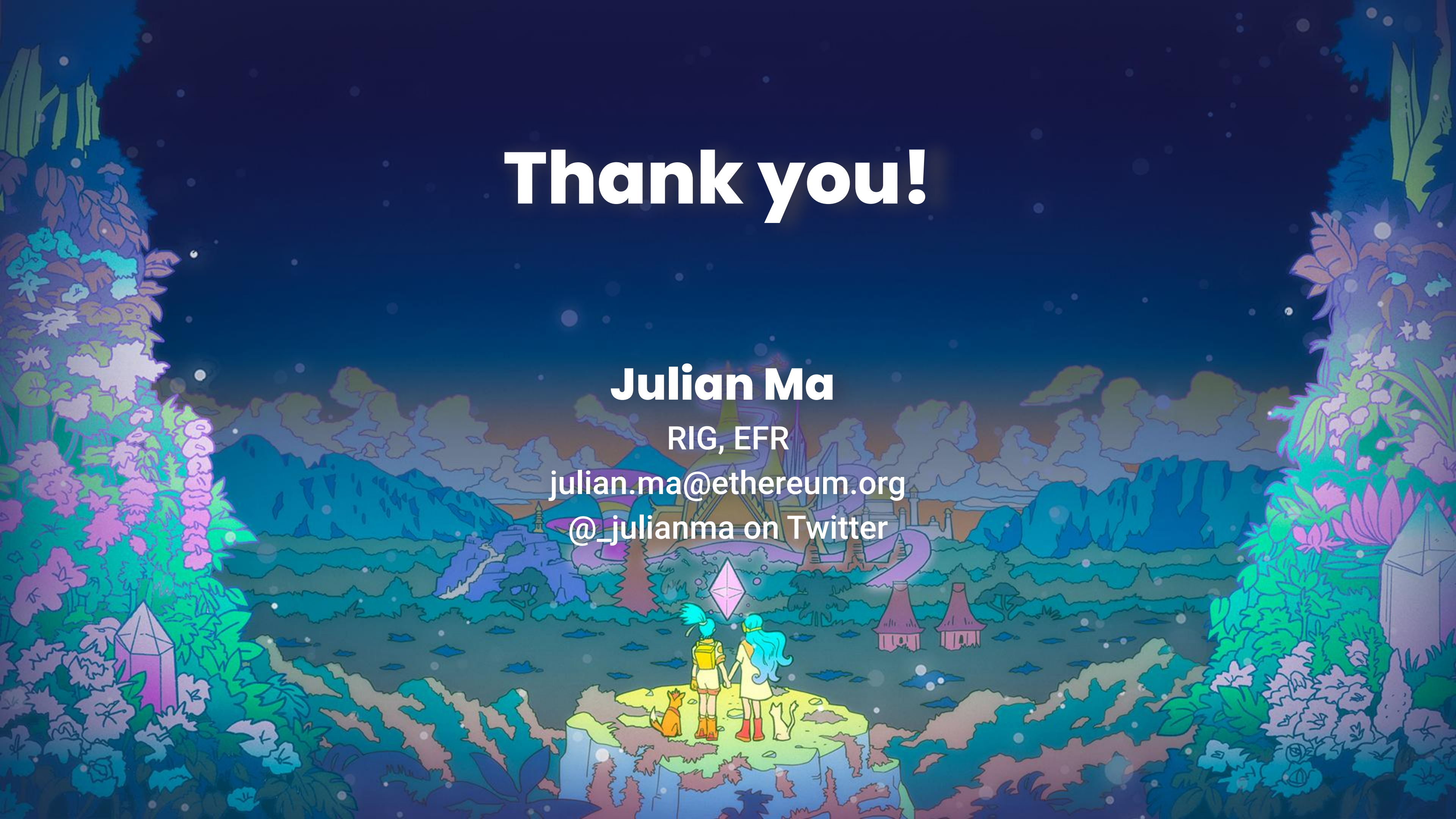
- Luckily not the case!
  - The dapp commits to its beliefs in a **sequential game, not simultaneously.**
- Commitment without regret.
  - The IL must be uncrowdable even though the commitment exists.
- Hence, there is no paradox.
  - **Even when applications specifically use uncrowdable inclusion lists, we can have uncrowdable inclusion lists!**

If the Censorship Resistance Gadget is Uncrowdable, then its creators can be decentralized.

If the Censorship Resistance Gadget is Crowdable, then its creators will be centralized.

Uncrowdable Censorship Resistance Gadgets seem Stable.

Thank you!



Julian Ma

RIG, EFR

julian.ma@ethereum.org

@_julianma on Twitter