FOCIL (EIP-7805)

Thomas Thiery, Francesco D'Amato, Julian Ma, Barnabé Monnot, Terence Tsao, Jacob Kaufmann, Jihoon Song

Julian Ma

Robust Incentives Group,
Ethereum Foundation

Inclusion List Design Philosophy

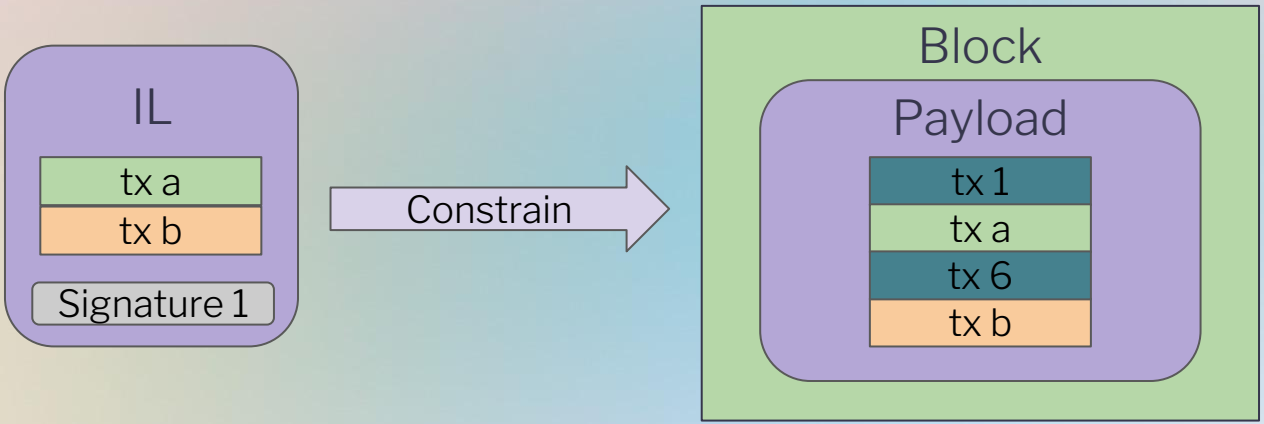
Inclusion Lists enable the most **decentralized** set of Ethereum participants to **provide inputs** into centralized block construction.

- **ILs leverage PBS**: Decentralized validators provide input into centralized block construction.

Necessary for Ethereum to retain core property of ✨ **Chain Neutrality** ✨.

Basic Inclusion List Idea

- There is a list of transactions that **constrains** the block in some way
- FOCIL is about:
  - **Who creates** these lists.
  - How are these lists **enforced**.



What are FOCIL's core properties?

Fork-**C**hoice enforced **I**nclusion **L**ists (FOCIL) allows **multiple validators** to provide inputs into block construction.

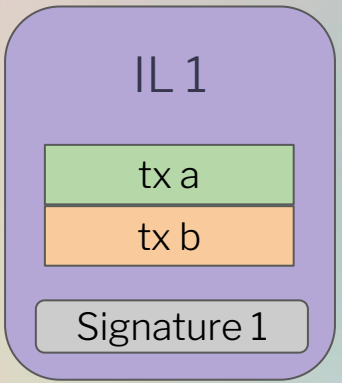
- Core property: **Increase Credible Neutrality.**

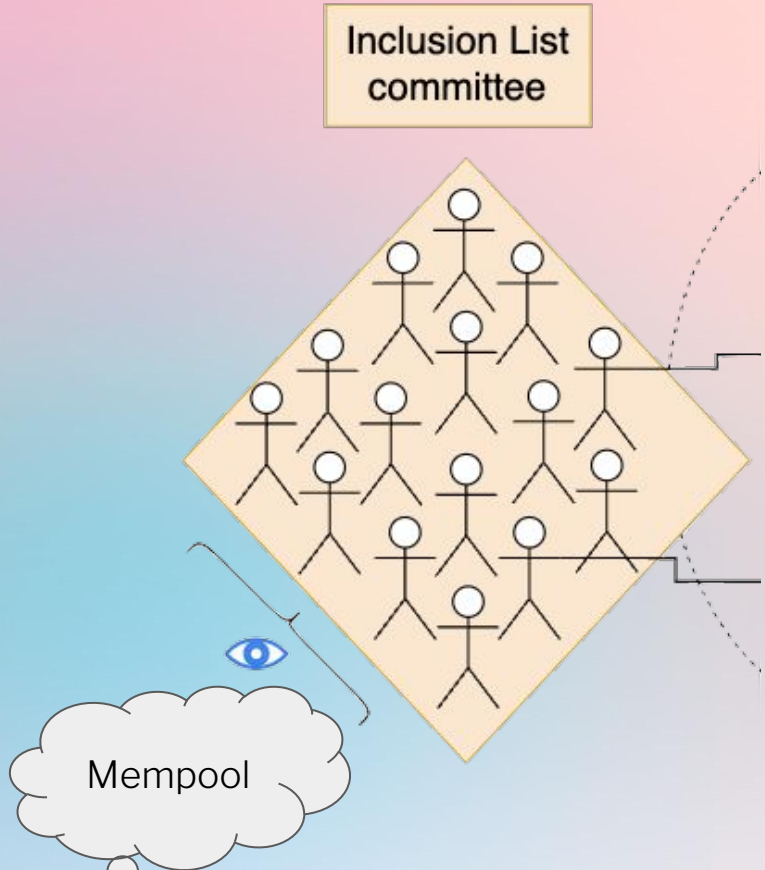
Other design goals:

- **Robustness**: FOCIL is used and only used for its intended purpose.
- **Extendability**: FOCIL is a **lightweight** mechanism extendable into different directions in the future.

Creating Inclusion Lists

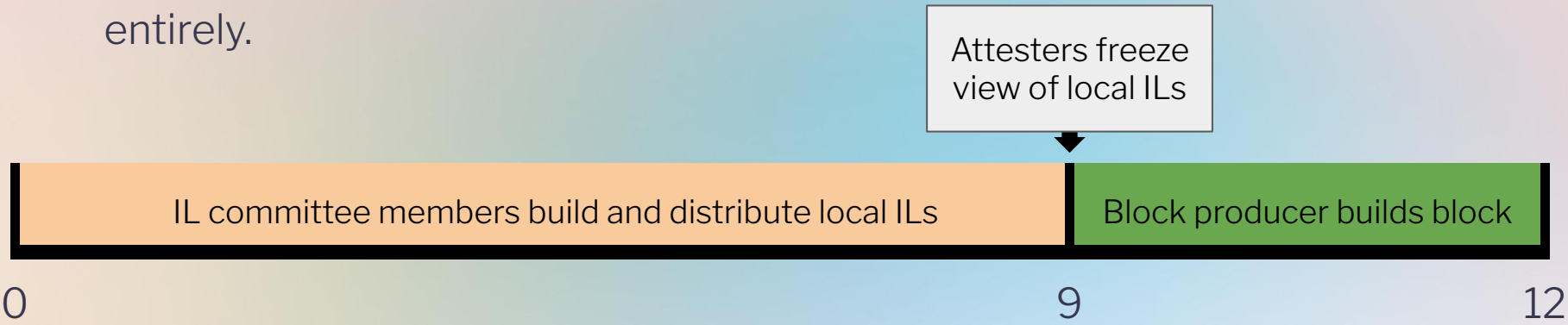
- Each slot, **16 validators** selected as IL committee members.
- Committee members observe mempool and construct IL.
- Each IL: 8kb or about 20 average txs.
- Total: about 320 average txs.





Distributing Inclusion Lists

- IL committee members distribute their IL over global topic as soon as they are made.
- 🧊 **Attesters** – who enforce the ILs – **freeze** 🧊 their view of available local ILs at second 9.
- The block producer has **3 seconds more** to see ILs and possibly retrieve them from attesters: **prevents split-view attack** ✋👀.
- **IL txs can be appended** to the execution payload: no need to rebuild block entirely.



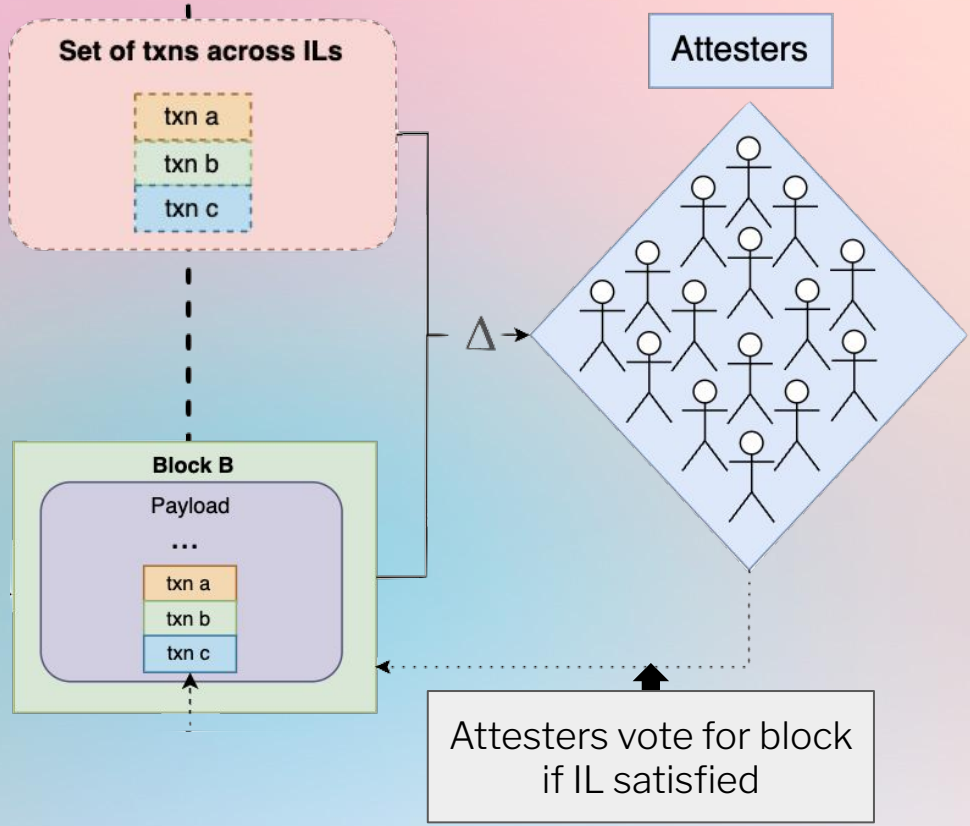
Enforcing the Inclusion List

- Enforcement via **Fo**rk-**C**hoice.
- Attester only votes for block if it satisfied the IL condition.

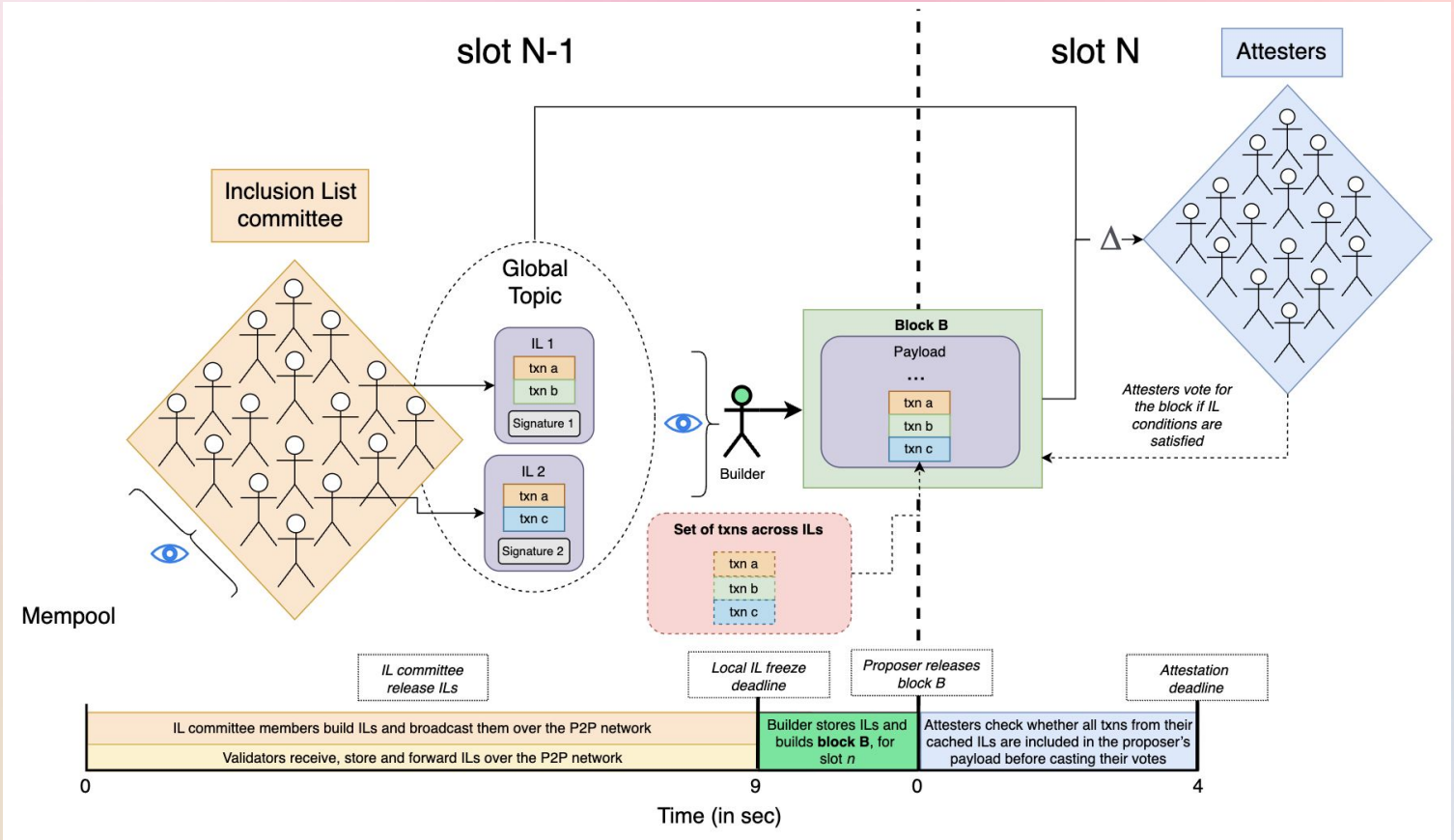
Condition in EIP-7805:

Block producer must include all txs from all ILs until the block is full.

- Conditional property.

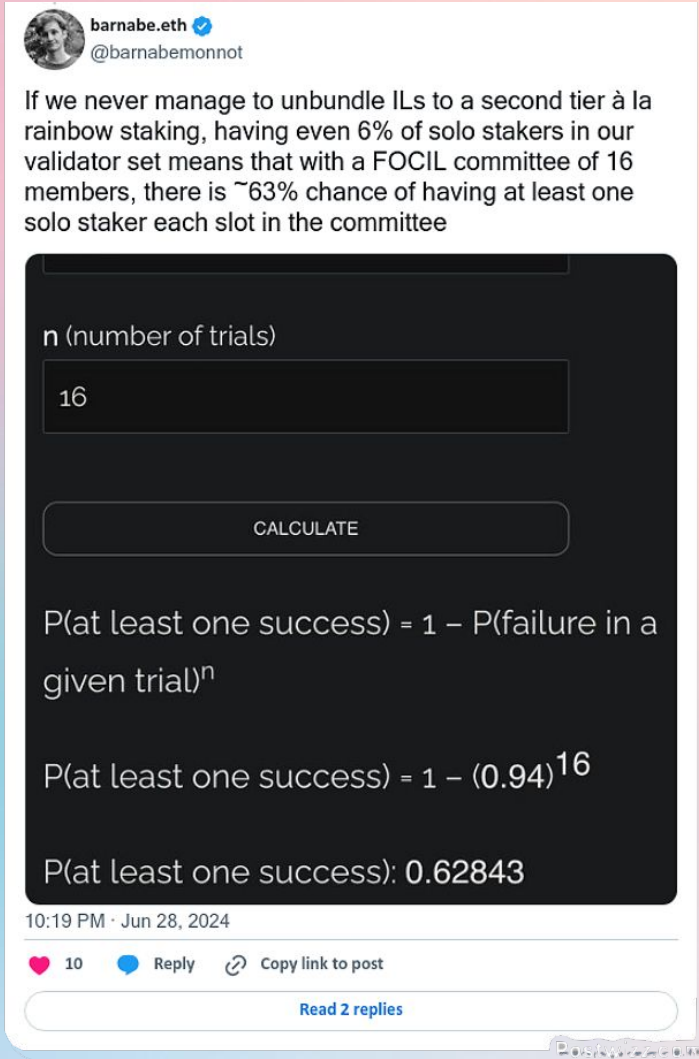


Full FOCIL Mechanism



Censorship Resistance Property

- **Only 1 honest** IL committee member needed for CR.
- With 6% solo stakers, there is a 63% chance of at least one solo staker in IL committee.
- **Boost signal provided by solo stakers** (leveraging PBS).
- EIP-7805 does not build on economic incentives for protocol simplicity.



Section 2

Robustness

IL Equivocation & Split-View

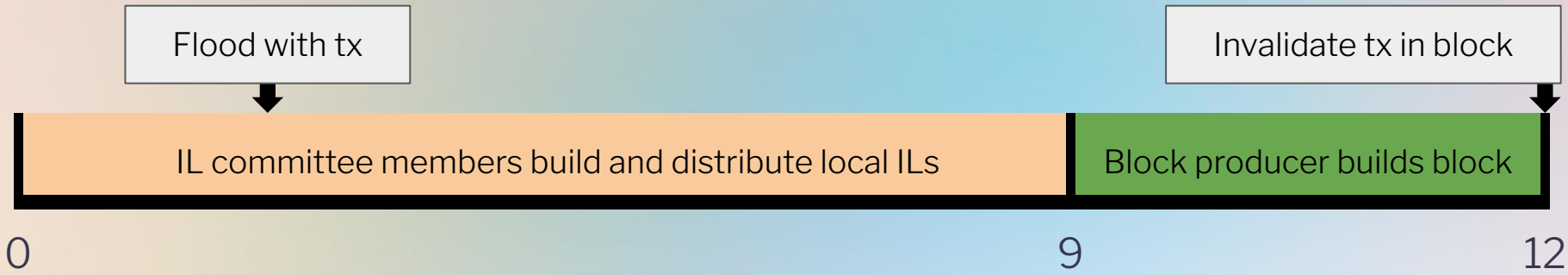
- **Split-view attacks** (🖖👀) are infeasible because the 🧊 **attesters freeze** 🧊 their view 3 seconds before the proposer does.
  - The proposer can request ILs from attesters if necessary.
- If a committee member **equivocates**:
  - Attesters propagate at most 2 ILs per committee member.
  - If an attester sees more than 1 IL per committee member, it ignores all ILs from this committee member.

Transaction Invalidation

- Txs included in an inclusion list may be **invalid** when the block producer must include them.
  - When IL proposers make inclusion lists, they may build on the **wrong head** of the chain.
  - AND, IL proposers **do not know** the execution payload of the upcoming block.
- To **prevent free DA**:
  - Attesters only check whether any IL tx not in the block could have been validly post-appended to the execution payload.
  - Inclusion lists are **not included on-chain**, but enforced via the fork-choice.

Robustness against invalid tx stuffing

- Txs in the IL may be invalid. Could an adversary **stuff** the IL with invalid transactions?
- Attack: Adversary **floods the mempool** with high-paying transactions which will be invalidated in the execution payload.
- Defense: **Diversity of ways IL proposers create ILs**.
  - By priority fee; By time tx is pending; Any other heuristic.
- Hard (and potentially costly) to attack all rules simultaneously.



Commitment Attacks

- **If** there were a single IL proposer, it could **extort** the block producer
  - **Unless the BP pays** the IL proposer a bribe, the IL proposer includes transactions the BP does not want included.
- **Multiple IL proposers** makes extortion attacks **very hard!**

- Similarly, bribing attacks are prevented.
  - IL proposer cannot ensure a transaction is only included if the BP pays the IL proposer, because other IL proposers may include the tx already!

IL-Boost / Uncrowdability

- Many previously worried a single IL proposer would **sell IL proposing rights.**
- **FOCIL is robust against MEV-Boost-like markets.**
  - No ordering guarantees.
  - Private order flow not possible.
  - Multiple IL proposers.
  - IL created 3 seconds before block producer acts.
- Individual IL proposer has no **inclusion, ordering or exclusion power.**

IL-Boost / Uncrowdability

- Many previously worried a single IL proposer would **sell IL proposing rights**.
  - Multiple IL proposers.
  - IL created 3 seconds before block producer acts.
- Individual IL proposer has no **inclusion, ordering or exclusion power.**

FOCIL is specifically designed to be robust against MEV markets for IL proposing rights.

Section 3

Extendability

Incentivize Censorship Resistance

- FOCIL **boosts the signal of solo stakers**, thereby contributing to censorship resistance.
- Some transactions may be actively **censored for economic reasons**, incentives can help here!
- **General idea: make it more expensive to censor transactions.**
- EIP-1559-like system for ILs: reward IL proposers who contribute to CR.
- Change tip system to incentivize CR.

FOCIL with Blobs

- EIP-7805 does not support blobs.
  - Although, with small changes potentially it could!™
- In a distributed block building world, **FOCIL could be extended to facilitate blobs.**
  - IL only enforced if attesters have a signal that the blobs in the IL must have been available to the BP.

FOCIL with Blobs

- EIP-7805 does not support blobs.
  - Although, with small changes potentially it could!™
- In a distributed block building world, **FOCIL could be extended to facilitate blobs.**
  - IL only enforced if attesters have a signal that the blobs in the IL must have been available to the BP.

FOCIL architecture is basis for many more extensions!

Summary

- FOCIL allows **16 extra validators** to contribute to block production!
  - Block production currently mostly in hands of 2 builders.
- Main goal: **increase censorship resistance of Ethereum.**
- Side goals:
  - **Robustness** against (MEV) attacks.
  - **Extendability**: FOCIL is architecture needed for future upgrades.

Next Steps

- **EIP-7805** is now available!
- Move towards implementation in clients.
- Reach out to us if...
  - You have questions.
  - You think you can use FOCIL as a vehicle for MEV.
  - You want to use FOCIL for your L2.

Thank you!

Julian Ma
Robust Incentives Group,
EF Research

julian.ma@ethereum.org