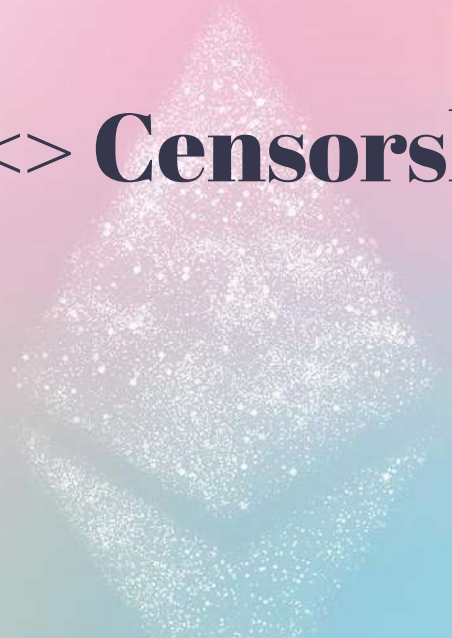
Statelessness <> Censorship Resistance



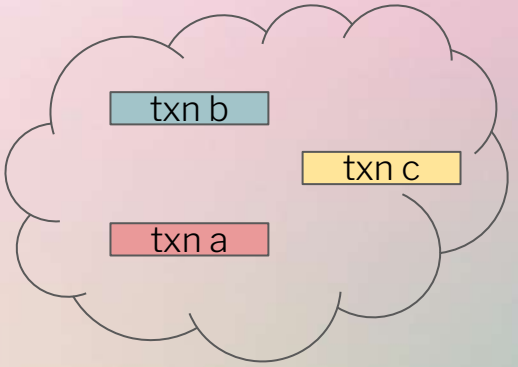
Thomas Thiery

@soispoke

Robust Incentives Group, Ethereum Foundation

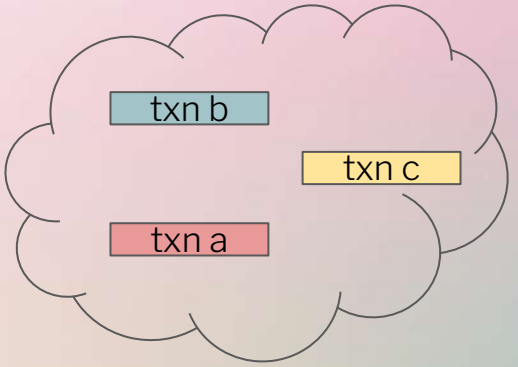
Censorship Resistance and Public Observability

Public Mempool



Censorship Resistance and Public Observability

Public Mempool



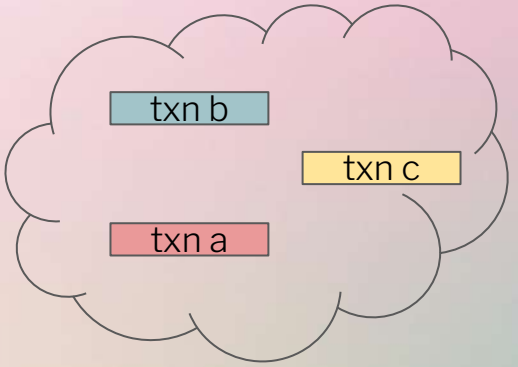
✅

Transaction validity assumption

nonce and balance checks

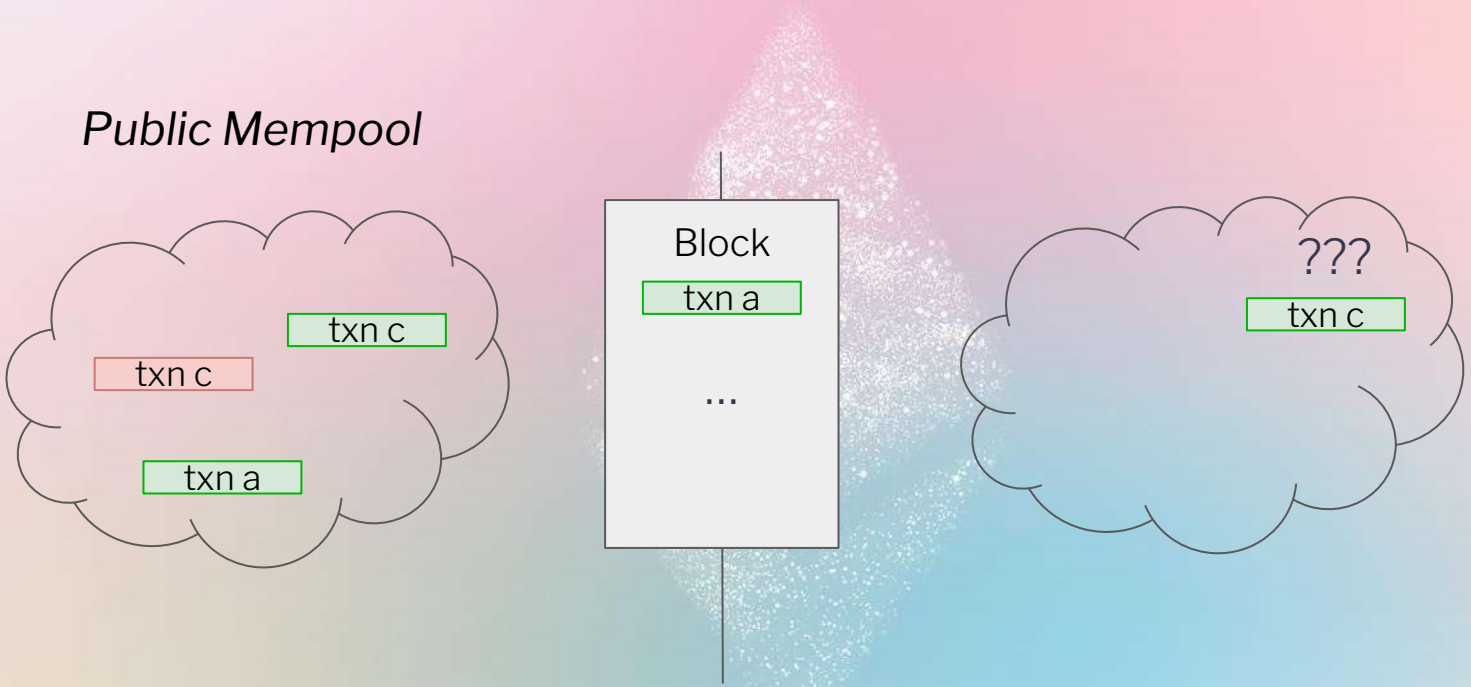
Censorship Resistance and Public Observability

Public Mempool



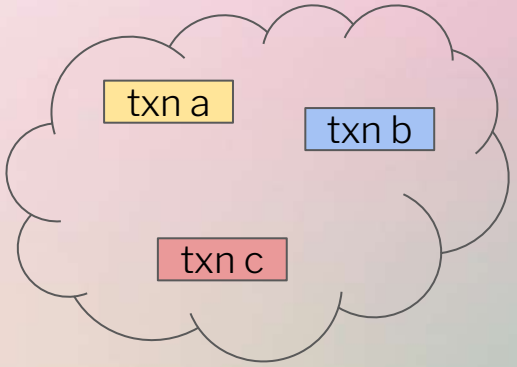
Time to inclusion

Censorship Resistance and Public Observability



Statelessness <> Censorship Resistance

Public Mempool



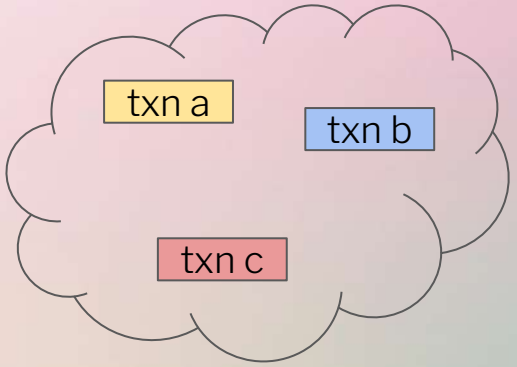
Stateful world 🌈🦄

✅ **Transaction validity assumption**

nonce and balance checks

Statelessness <> Censorship Resistance

Public Mempool



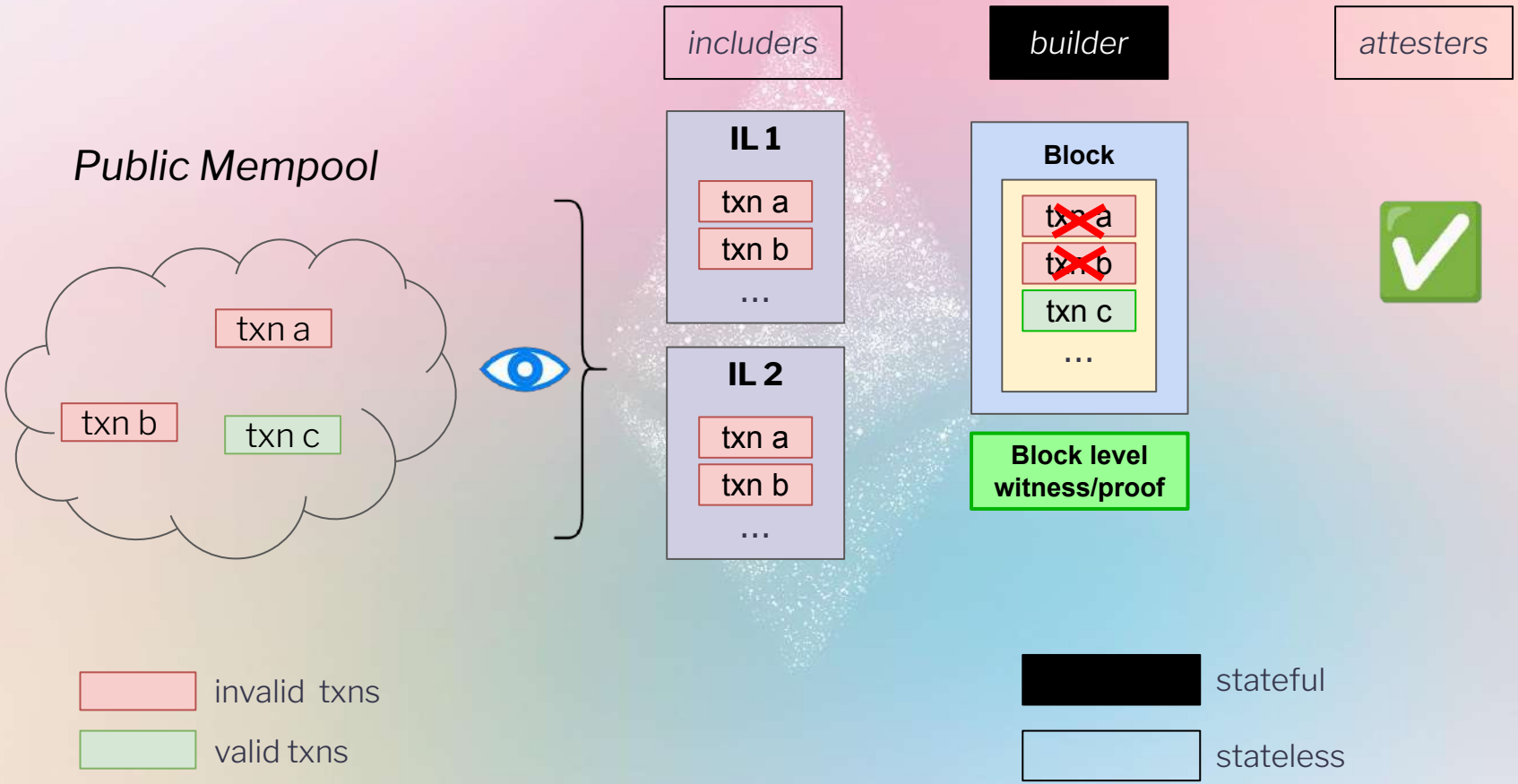
Stateless nodes

❌ **Transaction validity assumption**

nonce and balance checks

Statelessness <> FOCIL

Weak statelessness world



Statelessness <> FOCIL

Weak statelessness world

Issues:

- **IL flooding** 🌊🌊🌊
- Relying on **2 centralized builders?**

Statelessness <> FOCIL

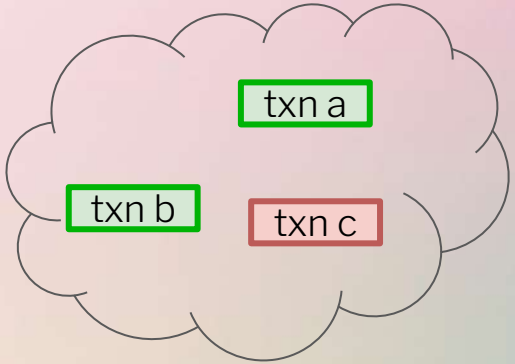
Strong statelessness world

includers

builder

attesters

Public Mempool



IL 1

txn a

txn b

...

IL 2

txn a

txn b

...

Block

txn a

txn b

...

Block level witness

invalid txns

valid txns

witness attached

stateless

Statelessness <> FOCIL

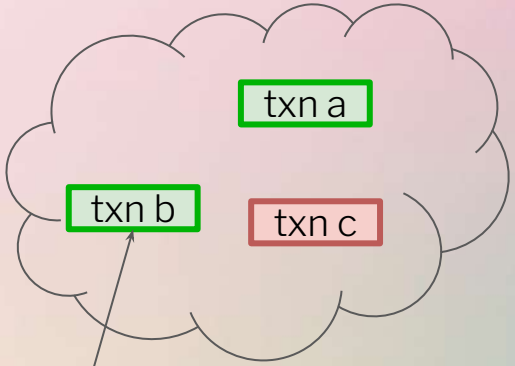
Strong statelessness world

includers

builder

attesters

Public Mempool



IL 1

txn a

txn b

...

IL 2

txn a

txn b

...

Block

txn a

txn b

...

Block level witness

invalid txns

valid txns

witness attached

stateful

stateless

Statelessness <> FOCIL

Strong Statelessness World

Issues:

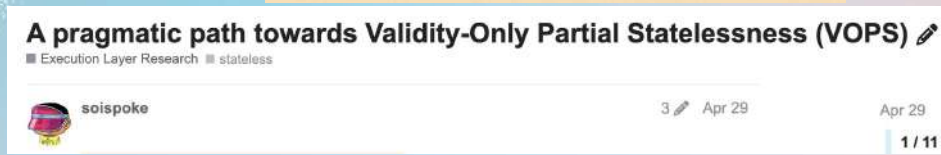
- **Who is responsible for holding the state and providing fresh witnesses?** Wallets? dApps? Portal? Supernodes (i.e., validators staking 2048 ETH)? All of the above?
- Witness stuffing 
- Degraded UX 💻⚙️

Validity-Only Partial Statelessness (VOPS)

- Nodes only store the minimal information needed to evaluate whether transactions should enter/remain in the mempool: **(address, nonce, balance, codeFlag) fields**

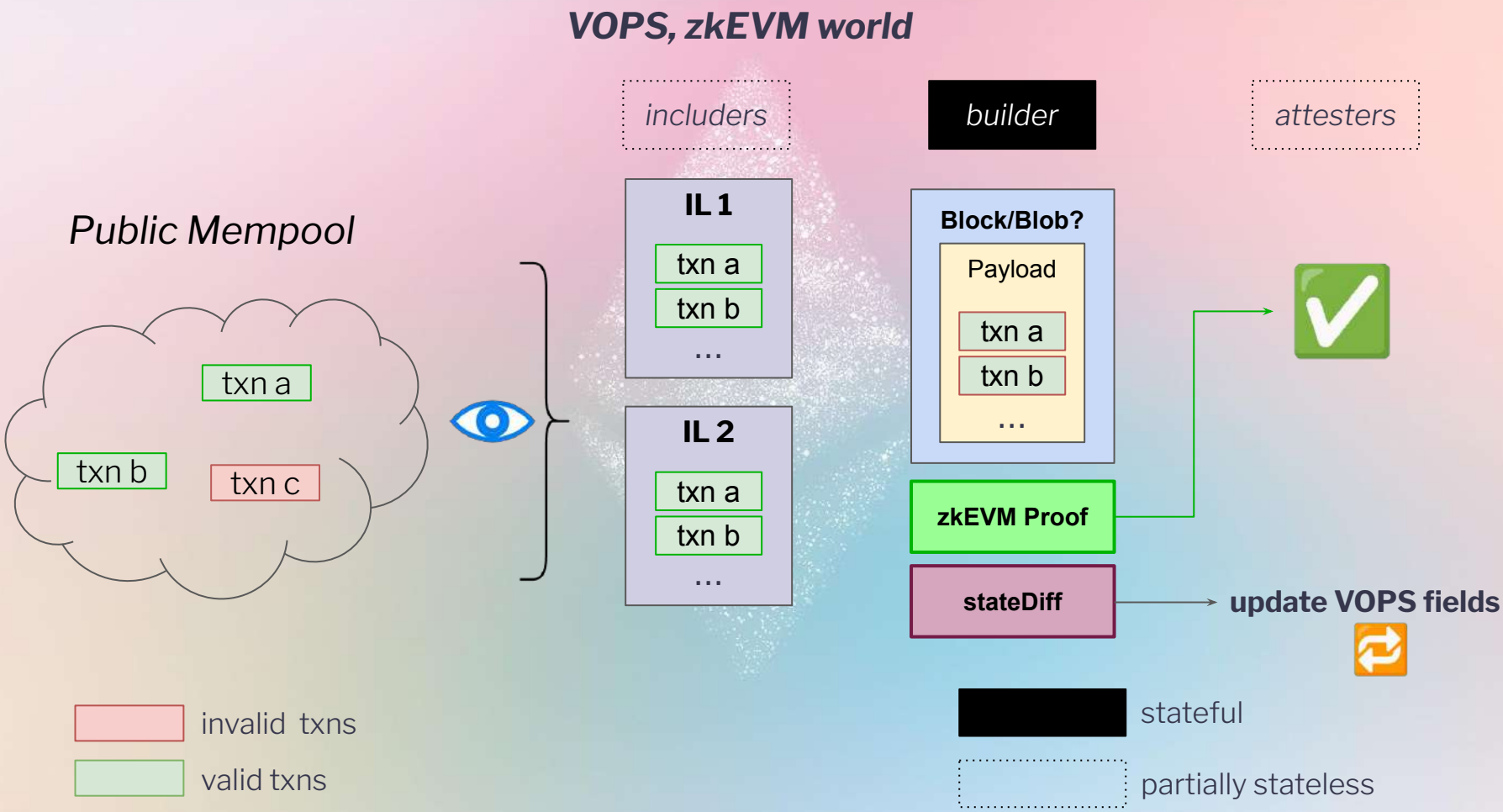
- This leads to a **25x reduction in storage** requirements for nodes today, from **233 GiB to 8 GiB**, while preserving the CR properties given by FOCIL.

- Works with zkVMs

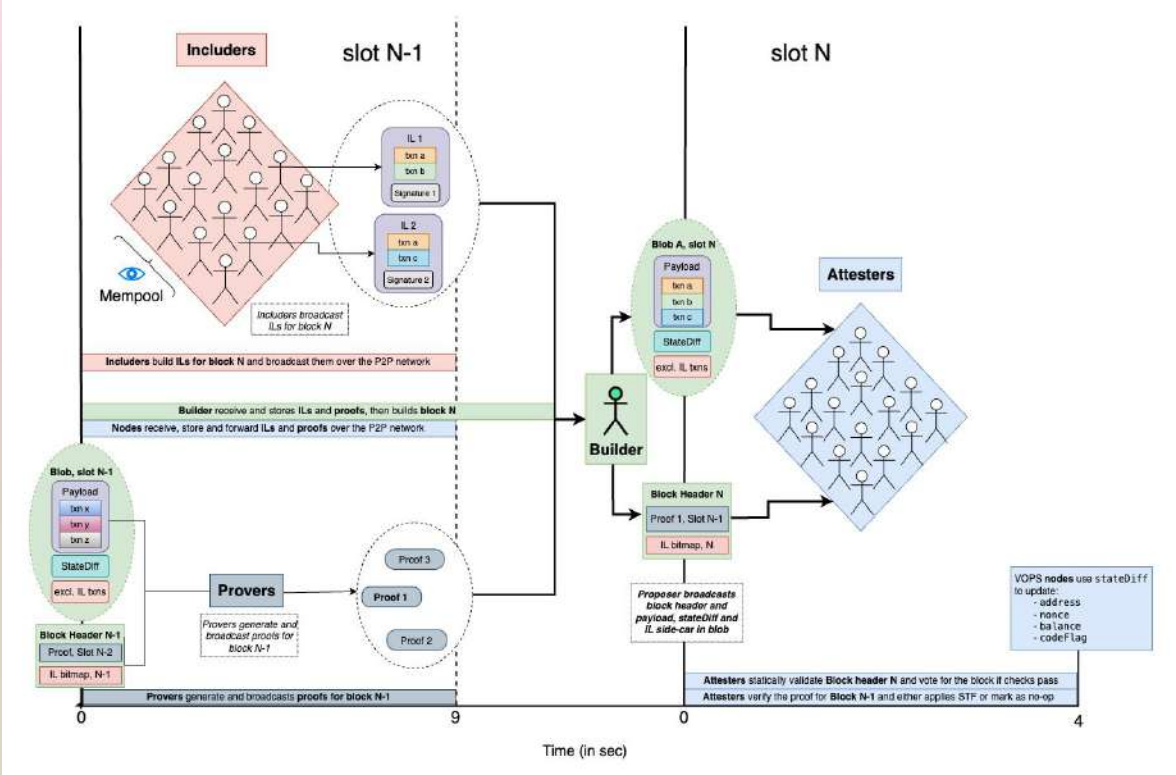


https://ethresear.ch/t/a-pragmatic-path-towards-validity-only-partial-statelessness-vops/22236

Validity-Only Partial Statelessness (VOPS)



Thank you!



https://hackmd.io/oE5LHy_CQL2PenT_803Axw?view