

The Ship of Theseus: efficient & long-lived ledgers

Can we *efficiently verify* distributed ledger state *despite dynamic membership*?

The setting:

- Permissioned ledger uses BFT to agree on state

The problem:

- Validator pool *changes over time*
- Need to traverse *entire history* to find transaction validators
- *Main goal*: validate blocks in $O(1)$ time

Approach:

- Use *proactive secret sharing* and *threshold signatures*
- Transactions verified with a *static public key*

