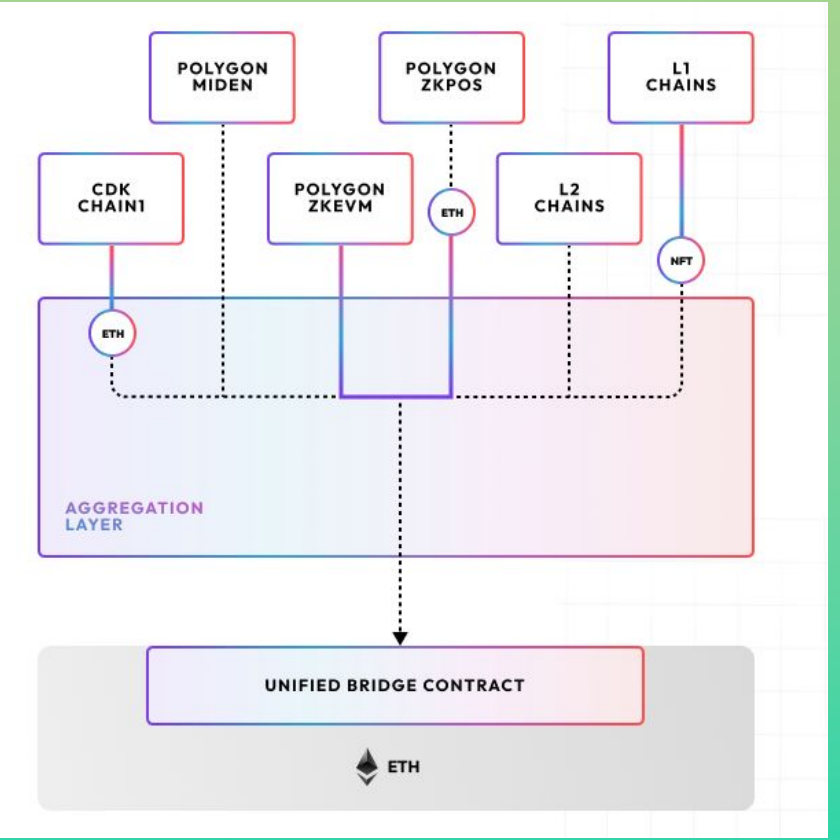
WTFrog is the pessimistic proof

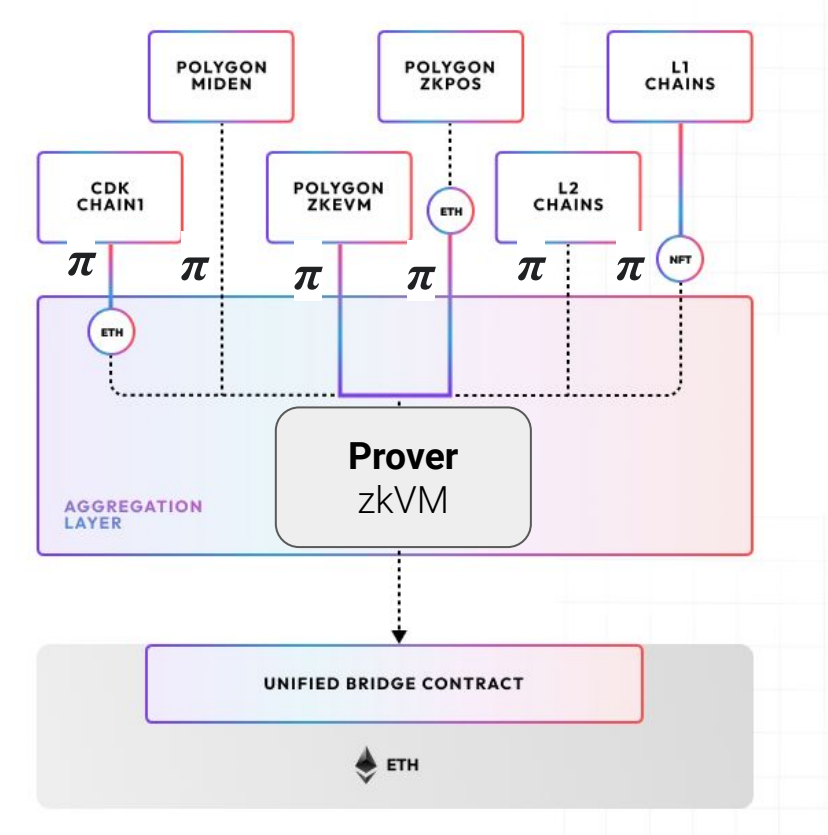
Ignasi Ramos
Polygon - Protocol team
@0xIgnasi

Aggregation Layer

The AggLayer connects sovereign chains together, unifying liquidity, users, and state, but with the feel of a single chain. A multichain web that is better for UX, better for network effects, and better for security.



The Pessimistic proof



The solution is to architect the Aggregation Layer in a way that assumes that every prover can be unsound. The Pessimistic Proof guarantees that even if a prover for a particular chain is unsound, that prover cannot drain more funds than are currently deposited on that chain. In this way, a soundness issue cannot infect the rest of the ecosystem.

Pessimistic proof computation

Leafs, exit roots, and Merkle trees

Local balance tree

- originNetwork
- tokenAddress
- balance

Local exit tree

- bridge exits

Nullifier tree

- Nullified bridges

Proof computation

1. Apply bridge exits to Old LET -> new LET
2. Apply bridge exits and imported bridge exits to old LBT -> new LBT
3. Check nullifiers
4. Check no negative balance in new LBT


Thank you!
Ignasi Ramos
Polygon - Protocol team
@0xIgnasi