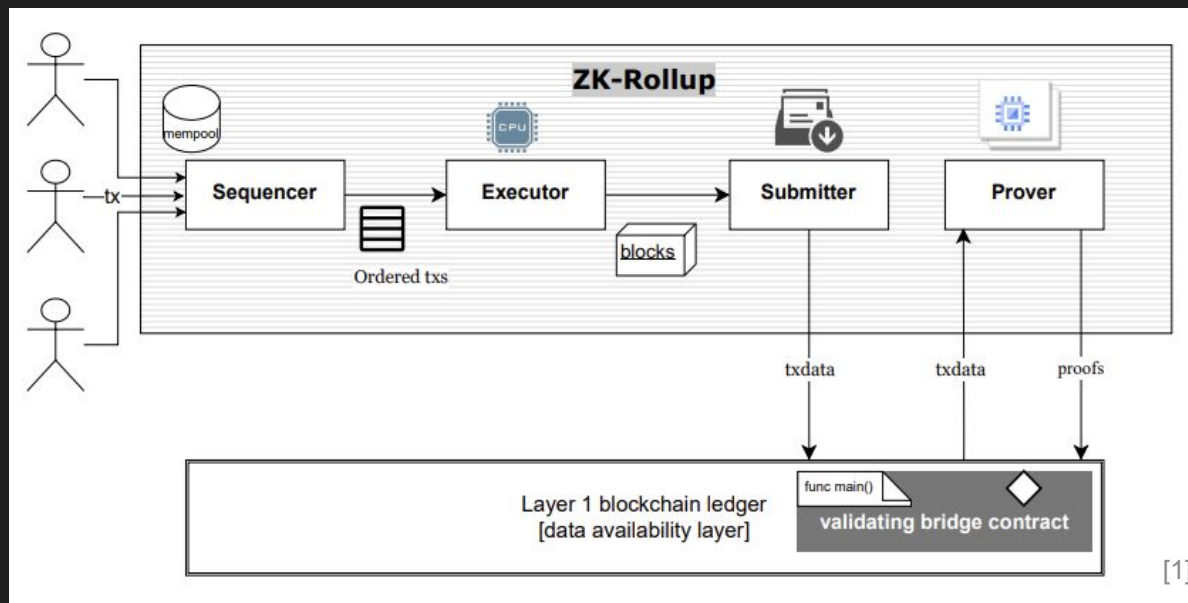


zkSharding: Scaling Ethereum with Sharded zkRollups

Handan K. Alper

zkRollups in a Nutshell

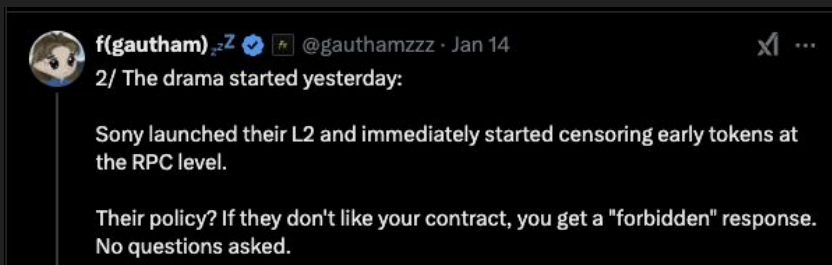


The Centralized Sequencer Problem in zkRollups

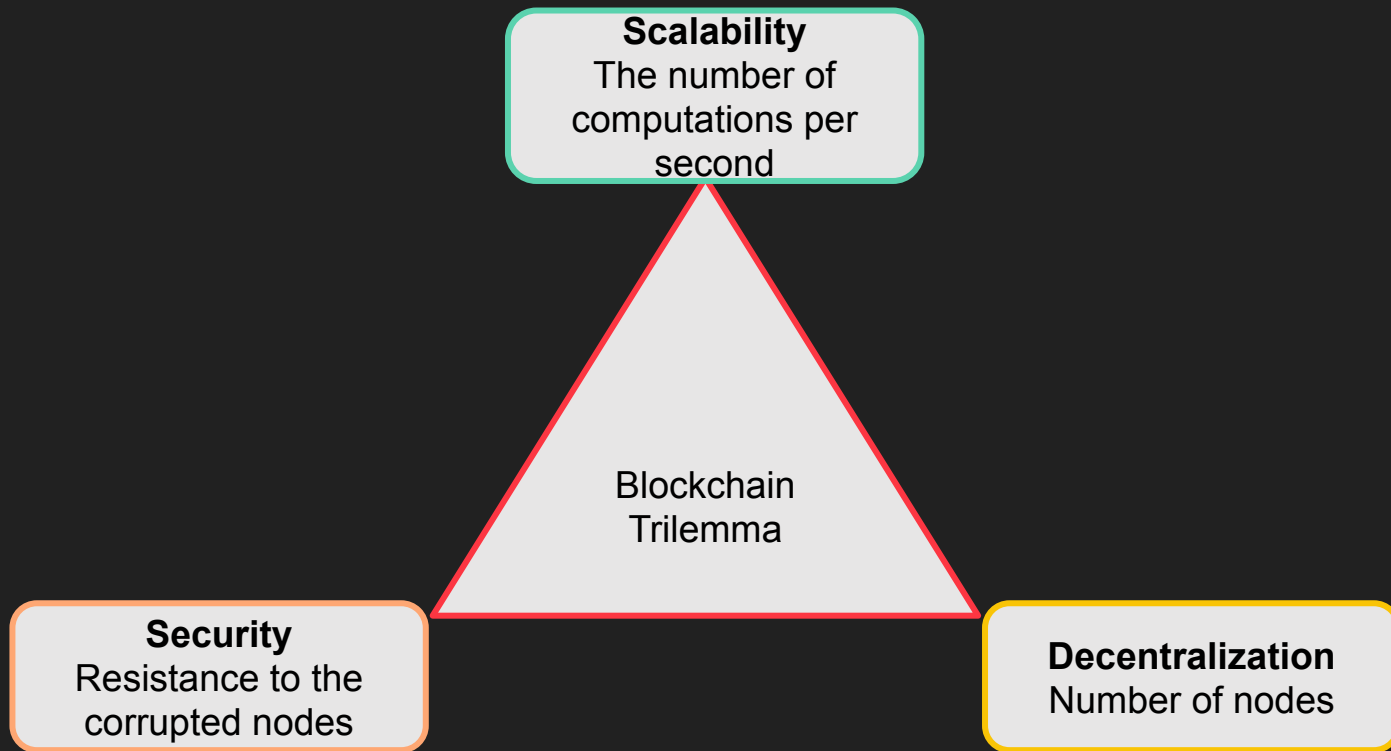
- Simplifies transaction ordering -> No complex consensus protocols needed
- Improves Performance and Throughput -> Efficient transaction processing
- Faster Iteration and Development -> Easier to implement and maintain

Ethereum Goal

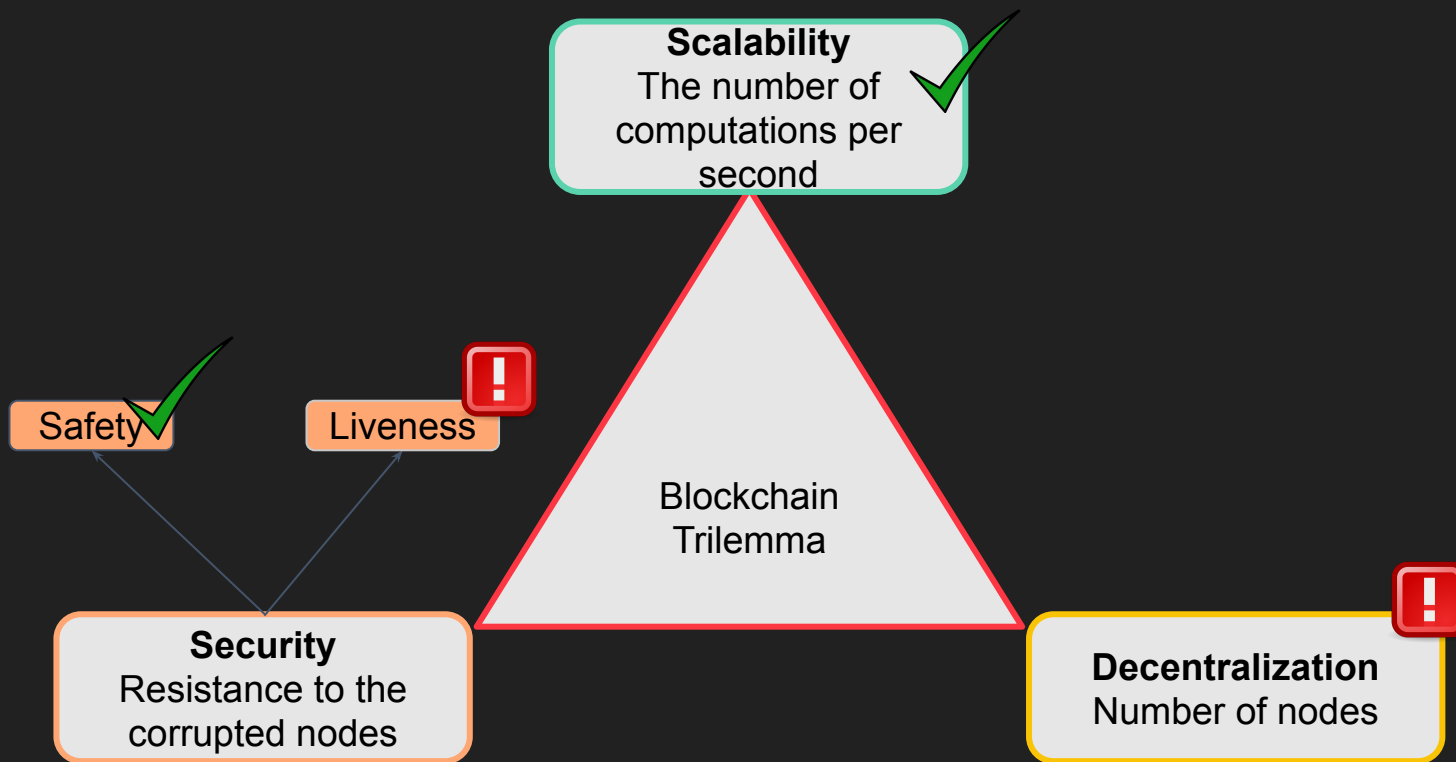
building a global, censorship-resistant permissionless blockchain



Blockchain Trilemma



Ethereum with a Centralized Layer 2



Ethereum - Layer 2 Dilemma

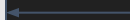
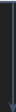
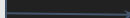


Scale Ethereum

Deploy Layer 2 Solutions

Scale Layer 2s

Decentralize Layer 2s



How can a Decentralized Layer 2 Scale?

Vertical Scaling

- Increase hardware requirements
 - centralization risk, reduce accessibility
 - scalability limits

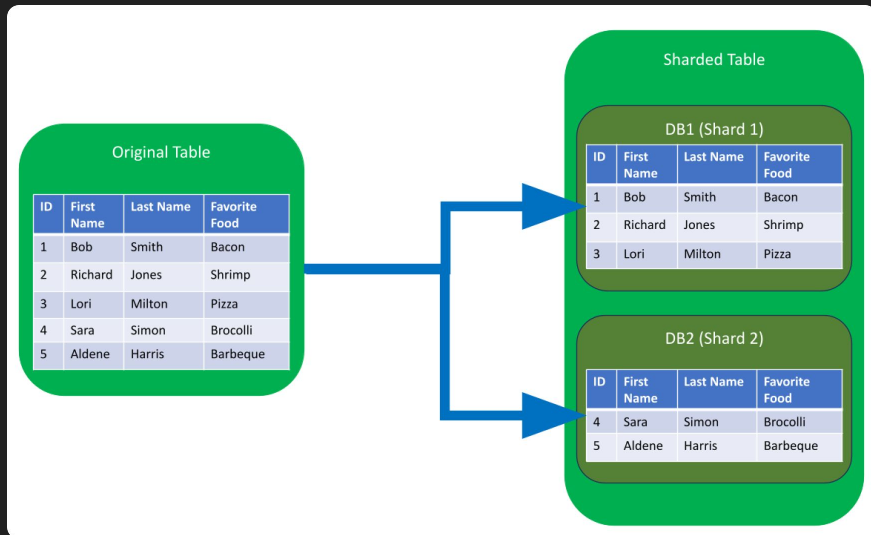
Horizontal Scaling



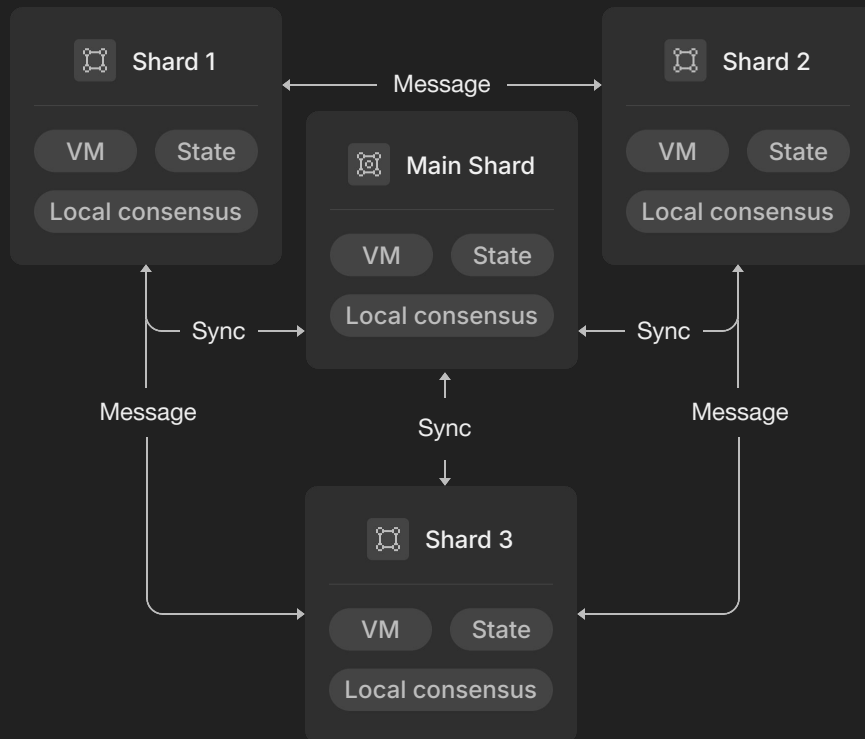
- Use multiple blockchains, distribute the amount of work
 - implementation complexity
 - interoperability between blockchains

Sharding

Classic DB sharding

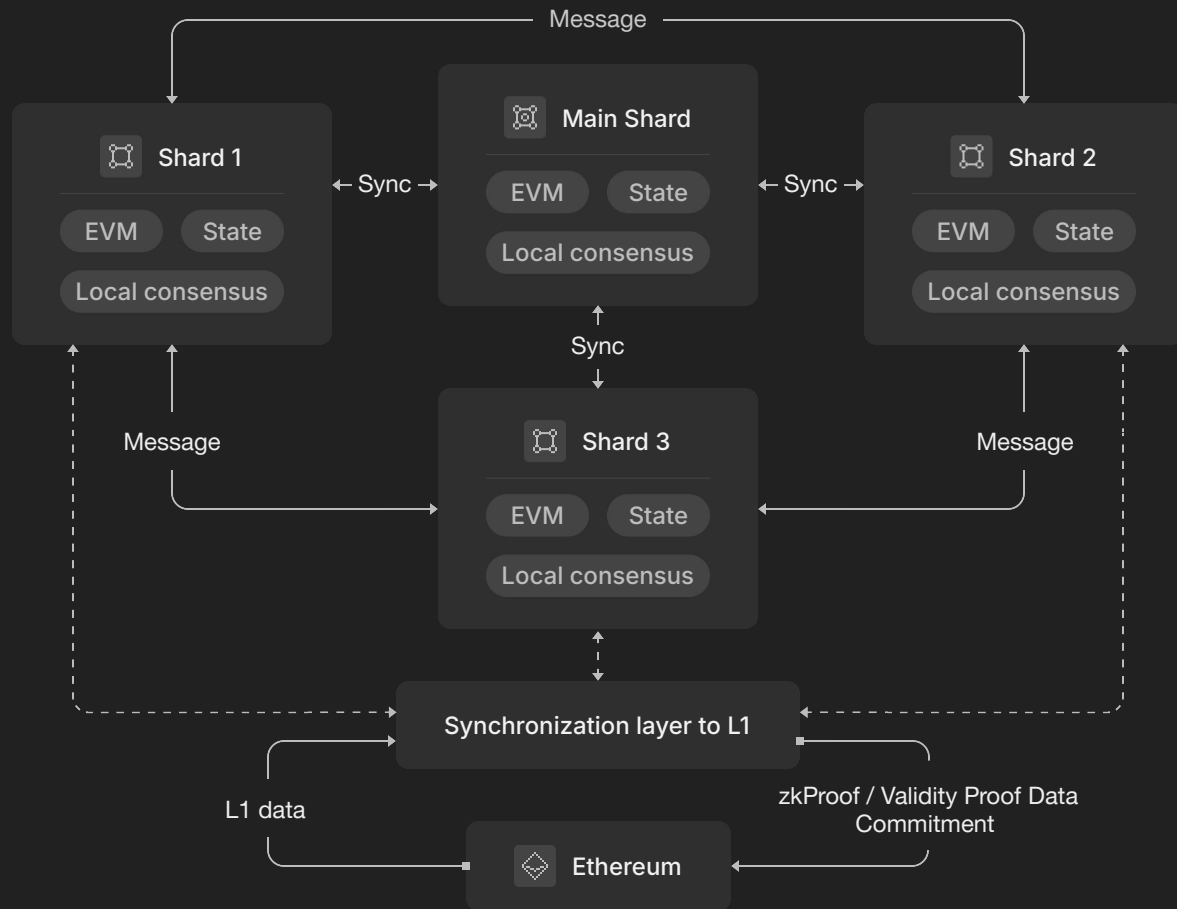


Decentralized network sharding



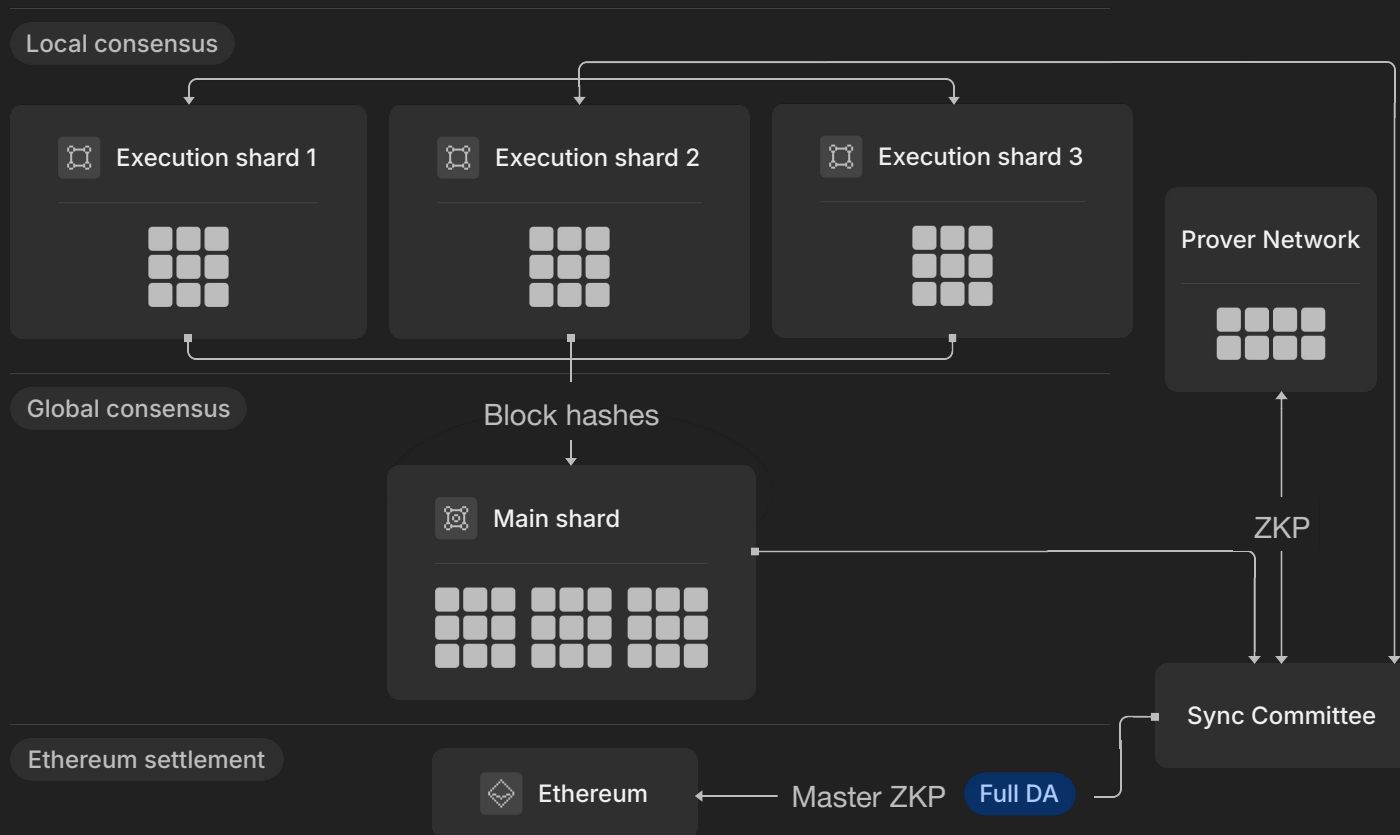
L2 Sharding

Ethereum is the settlement and data availability layer



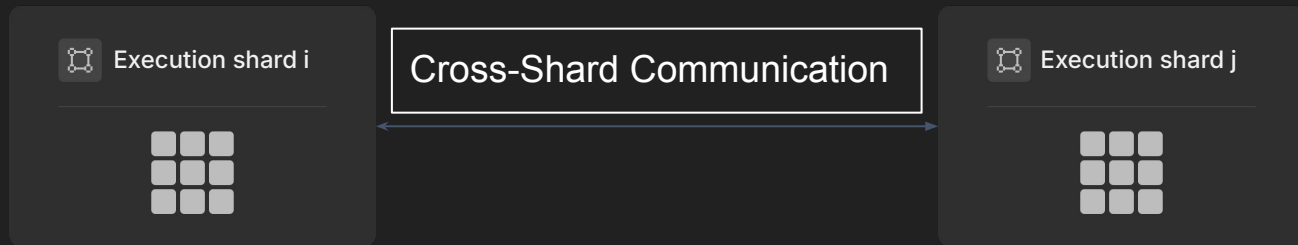
zkSharding

Sharded zkRollup
for parallel dApps
execution



Execution Shard

- Manage set of accounts
- Each account is managed by a smart contract
- Subset of validators are responsible for the local consensus of the execution shard



Cross Shard Communication

- **Non-atomic:** Transactions on the destination shard may be reverted, and smart contracts must handle these errors.
- **Optimistic:** Validators in the destination shard process transactions without waiting for zk-proof generation.
- **Permissionless:** Any shard can send transactions to other shards without additional setup.

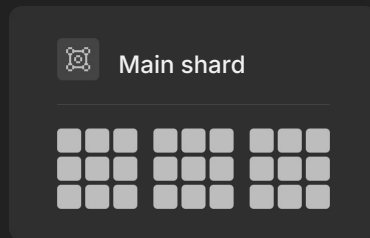
Inter-Chain Structure

DAG with Enforced Updates structure, where execution shards and the main shard are connected through **ShardDAG** rules:

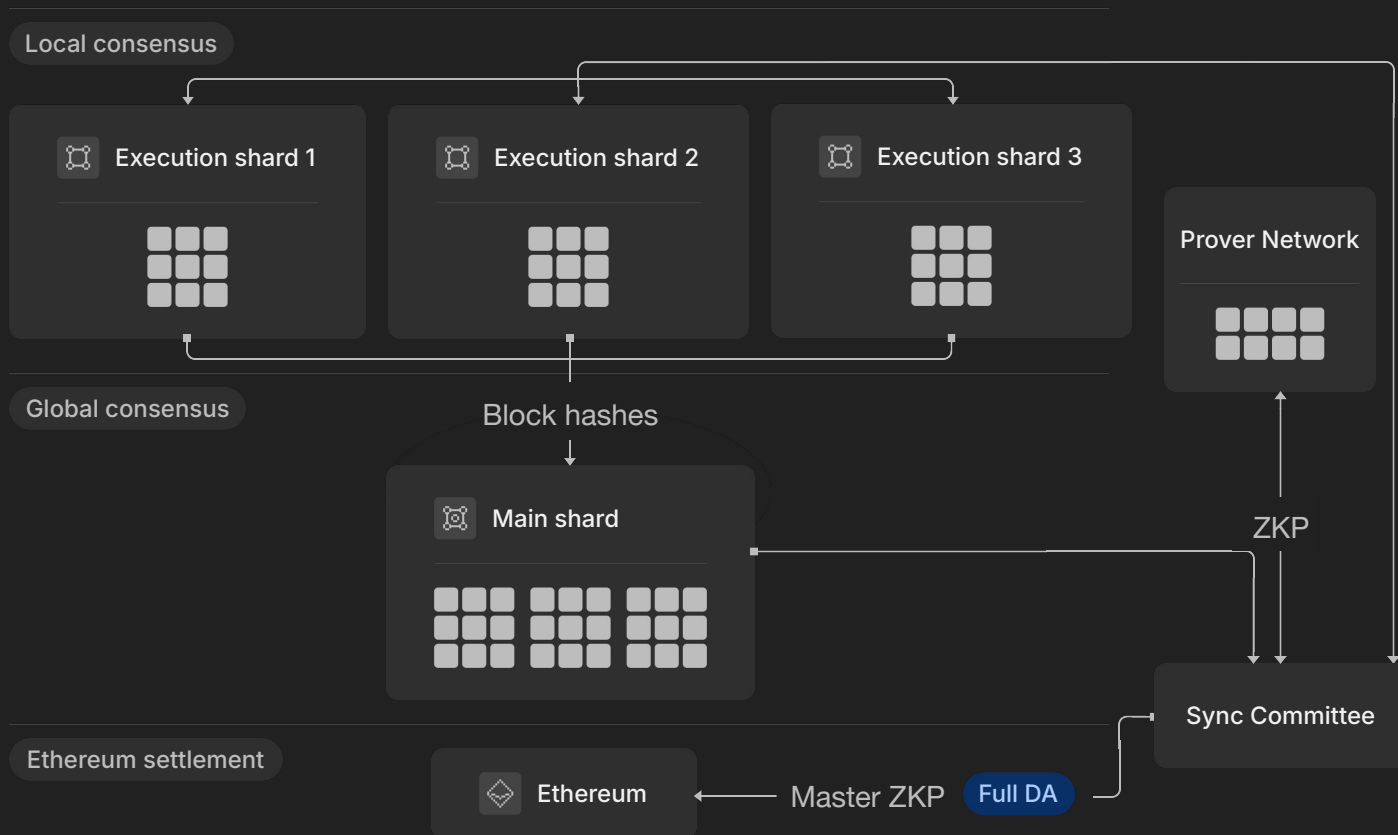
- Each block links to the previous block in its chain
- Each block references a previous block in the main shard
- Each block links to a set of blocks from other shards

Main Shard

- Responsible from operational executions:
 - Randomness generation
 - Staking and Slashing
 - Finalizing execution shard blocks
- All validators runs global consensus



Reaching Ethereum Finality



Properties Combinations



Thank you!

X: @handanKAlper

TG: @hndnklnc



<https://nil.foundation/>

X: @nil_foundation

zkSharding Consensus

