Scaling Blockchains

The quests discusses the challenges of scaling blockchains to handle higher transaction volumes and achieve mass adoption. It explains that simply increasing blockchain parameters like block size or gas limit (monolithic scaling) has limitations, as it requires nodes to have more storage, bandwidth, and computing power, reducing decentralization.

Full Nodes

Has full nodes allow to validate transactions and blocks to prevent consensus capture by malicious actors. Increasing resource requirements for full nodes reduces the number of entities able to run them, weakening the security model.

Modular approach to scaling

Involves unbundling the core functions of full nodes (execution, data availability, settlement) across separate layers or chains. This allows scaling by splitting computational work across multiple chains while still maintaining decentralization and security guarantees.

The modular approach envisions an execution layer for processing transactions, a data availability layer to ensure data is published, and a settlement layer to verify correct execution based on available data. This layered design aims to sustainably increase blockchain scalability without compromising core properties like decentralization and security.

Limits of Monolithic Scaling

- Even high-capacity monolithic chains run out of space as adoption grows
- They end up requiring fee markets and limiting throughput
- Pushing blockchain requirements reduces the number of full nodes backstopping security
- There are inherent trade-offs between scaling, decentralization and security

Modular Blockchain Architecture

- Unbundles the roles of a full node into separate layers/systems
- Execution Layer: Process transactions
- Data Availability Layer: Ensure data is published and available
- Settlement Layer: Verify correct execution based on available data
- Allows scaling by parallelizing work across specialized layers
- Retains security as each layer doesn't have to do all roles of a full node

Example: Chain Origin to Destination

- Destination doesn't need to be a full node that validates all Origin's state
- It just needs:
    1. Verification that assets originated from legitimate owners on Origin
    2. Guarantee that Origin's data is available to check claims

Benefits

- Modularity enables massive scaling by sharding trust
- Each layer can scale resources for its specific role
- Preserves decentralization as full node burdens are dispersed
- Enhances security from cross-layer verification

The key idea is divorcing blockchain computation from blockchain data and state availability to build scalable composable systems without centralization tradeoffs.