L41: Layer 2 Scaling Solutions

Module F: Advanced Topics

Blockchain & Cryptocurrency Course

December 2025

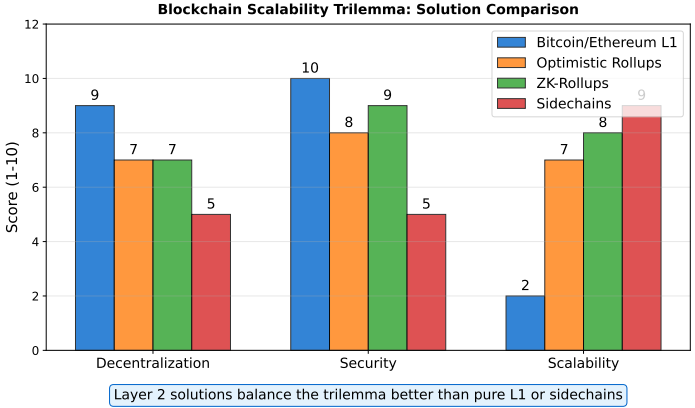
Learning Objectives

- Understand the blockchain scalability trilemma
- Compare Layer 2 design patterns (channels, rollups, sidechains)
- Analyze Optimistic vs ZK-Rollups tradeoffs
- Explore the Ethereum L2 ecosystem
- Evaluate the impact of Dencun upgrade (EIP-4844)

The Blockchain Scalability Trilemma

- **Trilemma**: Can only optimize 2 of 3 properties:
  1. **Decentralization**: Number of independent validators
  2. **Security**: Cost to attack the network
  3. **Scalability**: Transactions per second (TPS)
- Bitcoin: 7 TPS, Ethereum: 15 TPS
- Payment networks: Visa 65,000 TPS
- **Layer 2 Solutions**: Move transactions off-chain while inheriting L1 security

Trilemma Comparison by Solution



Rollups achieve better balance than L1 alone or sidechains

What is Layer 2?

Layer 1 (L1)

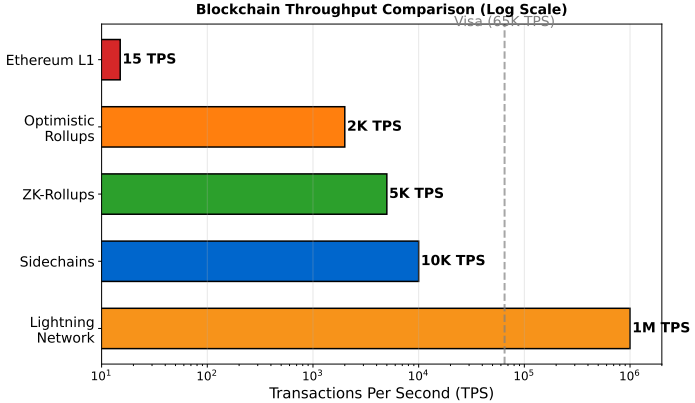
- Base blockchain protocol
- Full consensus for every transaction
- High security, low throughput
- Examples: Bitcoin, Ethereum

Layer 2 (L2)

- Built on top of L1
- Process transactions off-chain
- Settle final state on L1
- Inherit L1 security guarantees

Key Insight: Trade immediate finality for higher throughput

Throughput Comparison



L2s can match or exceed traditional payment networks like Visa

Layer 2 Design Patterns

1. **State Channels**: Direct peer-to-peer channels (Lightning Network)
2. **Sidechains**: Independent blockchains with two-way peg
3. **Rollups**: Batch transactions, compute off-chain, post data on-chain
   - Optimistic Rollups: Assume validity, allow fraud proofs
   - ZK-Rollups: Cryptographic validity proofs
4. **Plasma**: Hierarchical child chains with merkle commitments
5. **Validium**: Off-chain data availability + validity proofs

Lightning Network: Bitcoin's Layer 2

- **Problem**: Bitcoin's 7 TPS cannot support global payments
- **Solution**: Bidirectional payment channels
- **Mechanism**:
  1. Open channel with on-chain funding transaction
  2. Transact off-chain by updating channel state
  3. Close channel by broadcasting final state to L1
- **Network Topology**: Channels form payment routing graph
- **Capacity**: Millions of TPS, sub-second finality

Rollups: Ethereum's Scaling Strategy

- **Core Idea**: Execute transactions off-chain, post compressed data on-chain
- **Data Availability**: Transaction data published to L1
- **Computation**: Performed off-chain by sequencer/operator
- **State Roots**: Merkle root posted to L1 smart contract
- **Throughput**: 100-1000x improvement over L1
- **Two Variants**: Differ in how validity is proven

Optimistic Rollups

Mechanism

- Assume transactions valid by default
- Anyone can submit fraud proof
- Challenge period: 7 days
- If no challenge, state finalized

Advantages

- EVM compatibility (easy migration)
- Lower gas costs than L1

Fraud Proof System

- Verifier claims state is invalid
- Interactive bisection game on L1
- Dishonest party loses stake

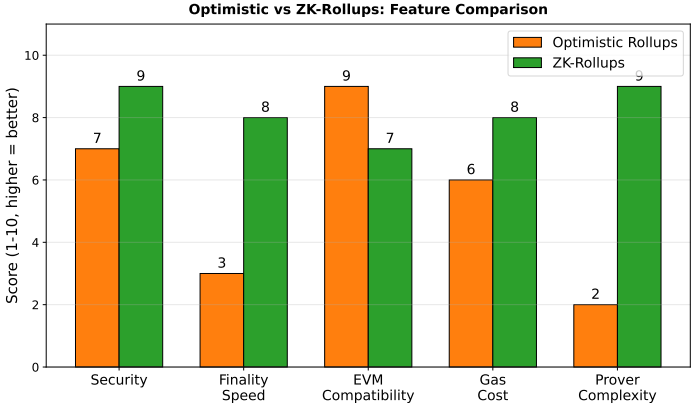
Disadvantages

- Long withdrawal delay (7 days)
- Honest verifier assumption

ZK-Rollups (Zero-Knowledge Rollups)

- **Mechanism**: Cryptographic validity proofs for every batch
- **SNARK/STARK Proofs**: Prove correct execution without revealing data
- **Verification**: L1 smart contract verifies proof (constant cost)
- **Finality**: Instant after proof verification (10-30 min)
- **Advantages**:
  - Fast withdrawals (no challenge period)
  - Stronger security guarantees
- **Disadvantages**:
  - Complex cryptography, higher prover costs
  - EVM compatibility challenges (improving)

Optimistic vs ZK-Rollups



ZK-Rollups excel in security and finality; Optimistic wins on EVM compatibility

Sidechains

Definition

- Independent blockchain with own consensus
- Two-way peg to main chain
- Assets locked on L1, minted on sidechain

Examples

- Polygon PoS (Ethereum)
- Liquid Network (Bitcoin)

Advantages

- Custom consensus rules
- High throughput, low fees

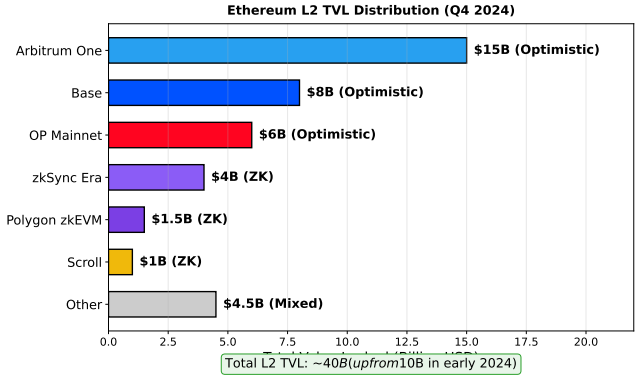
Disadvantages

- **Weaker security**: Does NOT inherit L1 security
- Trust in sidechain validators
- Bridge attack surface

Bridges: Connecting Chains

- **Purpose**: Transfer assets between L1 and L2, or across chains
- **Lock-and-Mint Pattern**:
  1. Lock assets on source chain
  2. Mint wrapped tokens on destination chain
  3. Burn wrapped tokens to unlock original
- **Bridge Types**:
  - **Trusted**: Centralized custodian (fast, low security)
  - **Federated**: Multi-sig operators
  - **ZK-Verified**: Cryptographic proofs (highest security)
- **Risk**: Bridges are major attack targets ($2B+ stolen in 2022-2023)

L2 TVL Distribution



Arbitrum leads by TVL; optimistic rollups currently dominate

2024: The Year of Layer 2 Explosion

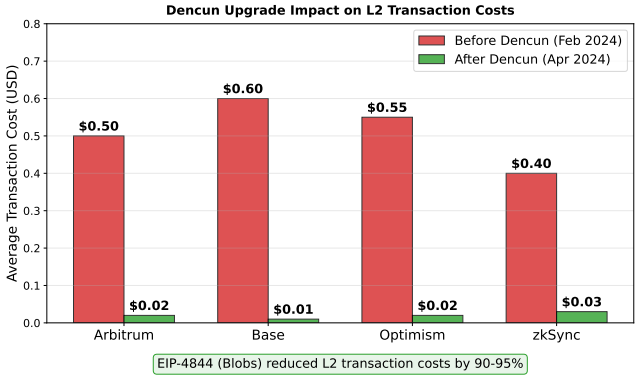
Dencun Upgrade Impact (March 2024):

- EIP-4844 blob transactions reduced L2 fees by 90%+
- L2 transaction costs: \$0.50-2.00 $\rightarrow$ \$0.01-0.05
- User migration to L2s accelerated dramatically

Key Trends:

- Combined L2 TVL: \$40B (up from \$10B in early 2024)
- Daily transactions: L2s now exceed Ethereum L1
- "App chains": Custom L2/L3s for specific applications
- ZK maturity: zkSync, Scroll, Linea gaining traction

Dencun Impact on L2 Fees



EIP-4844 blob transactions were the most significant scaling upgrade since the Merge

Security Comparison

Solution	Inherits L1 Security	Trust Model	Finality
Optimistic Rollup	Yes	1-of-N honest	7 days
ZK-Rollup	Yes	Cryptographic	10-30 min
State Channel	Yes	Counterparty online	Instant
Sidechain	No	Validator set	Chain-dependent

Key Takeaway: Rollups inherit L1 security; sidechains do not

Future Directions

- **Full Danksharding**: Massive data availability increase (100,000+ TPS)
- **zkEVM Maturity**: Fully EVM-equivalent ZK-rollups
- **Layer 3**: Application-specific rollups on top of L2
- **Interoperability**: Cross-rollup communication protocols
- **Sequencer Decentralization**: Remove single point of failure
- **Shared Sequencing**: Multiple rollups share infrastructure

Summary

Key Takeaways:

- Layer 2 solutions scale blockchains while preserving decentralization
- **State Channels**: Peer-to-peer, instant finality (Lightning)
- **Optimistic Rollups**: Fraud proofs, 7-day withdrawal, EVM-compatible
- **ZK-Rollups**: Validity proofs, fast finality, high security
- **2024 Milestone**: Dencun/EIP-4844 made L2s 10x cheaper
- **Current Landscape**: Arbitrum, Optimism, Base lead; ZK maturing
- **Future**: Multi-layered ecosystem with app-specific L2s/L3s

Questions for Reflection

1. Why do optimistic rollups have a 7-day withdrawal delay?
2. What makes ZK-rollups more secure than optimistic rollups?
3. Why don't sidechains inherit Layer 1 security?
4. How did EIP-4844 reduce L2 transaction costs so dramatically?
5. What are the tradeoffs between using an L2 vs. a sidechain?