

L41: Layer 2 Scaling Solutions

Module F: Advanced Topics

Blockchain & Cryptocurrency Course

December 2025

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 Layer 1 security

What is Layer 2?

Layer 1 (L1)

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

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

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

- **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

Opening a Channel

- Alice and Bob create 2-of-2 multisig
- Fund with on-chain transaction
- Initial state: Alice 0.5 BTC, Bob 0.5 BTC

Updating State

- Alice pays Bob 0.1 BTC off-chain
- New state: Alice 0.4 BTC, Bob 0.6 BTC
- Both sign commitment transaction
- No blockchain interaction

Closing Channel

- Cooperative close: broadcast final state
- Unilateral close: either party can exit
- Timelock + revocation keys prevent cheating

Routing Payments

- Alice pays Carol via Bob's channel
- Hash Time-Locked Contracts (HTLCs)
- Atomic multi-hop payments

- **Penalty Mechanism:** Publishing old state results in fund loss
- **Watchtowers:** Monitor blockchain for fraudulent channel closes
- **Timelocks:** Dispute period for fraud proofs
- **Limitations:**
 - Both parties must be online to transact
 - Liquidity locked in channels
 - Routing path finding complexity
 - Capital efficiency vs connectivity tradeoff
- **Current Status:** 5,000 BTC capacity (\$200M), 15,000+ nodes

- **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

Mechanism

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

Advantages

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

Fraud Proof System

- Verifier claims state root is invalid
- Interactive bisection game on L1
- Execute disputed transaction on L1
- Dishonest party loses staked funds

Disadvantages

- Long withdrawal delay (7 days)
- Honest verifier assumption
- Capital inefficiency during dispute period

- **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
 - Higher throughput (less data posted)
- **Disadvantages:**
 - Complex cryptography
 - Higher prover costs (specialized hardware)
 - EVM compatibility challenges (improving)

Optimistic vs ZK-Rollups Comparison

Property	Optimistic	ZK-Rollup
Validity Assumption	Optimistic (fraud proofs)	Cryptographic proofs
Withdrawal Time	7-14 days	10-30 minutes
EVM Compatibility	Native	Requires zkEVM
Gas Costs	Medium	Low (less data)
Prover Complexity	Low	High (SNARK/STARK)
Security Model	1-of-N honesty	Cryptographic
Examples	Arbitrum, Optimism	zkSync, StarkNet, Polygon zkEVM

Trend: ZK-Rollups gaining adoption as zkEVM matures

Definition

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

Examples

- Polygon PoS (Ethereum sidechain)
- Liquid Network (Bitcoin sidechain)
- Ronin (Axie Infinity)

Advantages

- Custom consensus rules
- High throughput
- Low transaction fees
- Flexibility in design

Disadvantages

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

- **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 assets
- **Bridge Types:**
 - **Trusted:** Centralized custodian (fast, low security)
 - **Federated:** Multi-sig operators (medium trust)
 - **Optimistic:** Fraud proof system
 - **ZK-Verified:** Cryptographic proofs (highest security)
- **Risk:** Bridges are major attack target (\$2B+ stolen in 2022-2023)

- **Challenge:** How to verify L2 state without full transaction data?
- **Rollup Requirement:** Post transaction data to L1 (expensive)
- **Validium Approach:** Store data off-chain, only post state roots
 - Higher throughput, lower costs
 - Trust assumption: Data availability committee
- **Data Availability Sampling (DAS):** Light clients randomly sample data chunks
- **Future Solutions:** EIP-4844 (Proto-Danksharding) – dedicated blob space for rollups

- **Ethereum L2s:**

- Optimistic: Arbitrum (\$10B TVL), Optimism (\$6B TVL), Base
- ZK-Rollups: zkSync Era, Polygon zkEVM, StarkNet, Scroll
- Sidechains: Polygon PoS (\$5B TVL)

- **Bitcoin L2s:**

- Lightning Network (payment channels)
- Rootstock (EVM sidechain)
- Stacks (smart contracts via Bitcoin finality)

- **Total L2 TVL:** \$40B (as of Q4 2024)

- **Trend:** Multi-chain future with specialized L2s

Security Comparison Table

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 (unilateral exit)
Sidechain	No	Validator set	Chain-dependent
Validium	Partial	Data committee	10-30 min

Key Takeaway: Rollups inherit L1 security; sidechains do not

- **Ethereum L1:** 15 TPS, \$1-\$50 per transaction
- **Optimistic Rollups:** 1,000-4,000 TPS, \$0.10-\$1 per transaction
- **ZK-Rollups:** 2,000-10,000 TPS, \$0.05-\$0.50 per transaction
- **Sidechains:** 5,000-20,000 TPS, \$0.001-\$0.10 per transaction
- **Lightning Network:** Millions of TPS, \$0.0001-\$0.001 per transaction
- **Tradeoff:** Higher throughput often means weaker security guarantees

- **EIP-4844 (Proto-Danksharding):** Blob transactions for cheaper rollup data
- **Full Danksharding:** Massive data availability increase (target: 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 sequencer infrastructure

Dencun Upgrade Impact (March 2024):

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

L2 TVL and Activity (Late 2024):

- Combined L2 TVL: \$40B (up from \$10B in early 2024)
- Daily transactions: L2s now exceed Ethereum L1
- Base (Coinbase): Fastest growing, \$3B+ TVL
- Arbitrum: Largest by TVL (\$15B), strongest DeFi ecosystem
- Optimism: Superchain vision, multiple OP Stack chains

Key Trends:

- “App chains”: Custom L2/L3s for specific applications
- Superchain: Shared sequencer, cross-L2 interoperability
- ZK maturity: zkSync, Scroll, Linea gaining traction
- Centralized sequencers remain (decentralization roadmap ongoing)

- **Layer 2 solutions scale blockchains while preserving decentralization**
- **State Channels:** Peer-to-peer, instant finality (Lightning Network)
- **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
- **Bridges:** Critical infrastructure with significant attack surface
- **Current Landscape:** Arbitrum, Optimism, Base lead; ZK rollups maturing
- **Future:** Multi-layered ecosystem with app-specific L2s/L3s