

L41: Layer 2 Scaling Solutions

Module F: Advanced Topics

Blockchain & Cryptocurrency Course

December 2025

- Describe the blockchain scalability trilemma
- Compare Layer 2 design patterns (channels, rollups, sidechains)
- Analyze Optimistic vs ZK-Rollups tradeoffs
- Evaluate the impact of Dencun upgrade (EIP-4844)
- Explain Account Abstraction (ERC-4337) and its UX improvements

The Problem: How do we scale without sacrificing security?

The Challenge

Ethereum can only process 15 transactions per second, while Visa handles 65,000 TPS. Traditional scaling approaches (increasing block size, reducing block time) sacrifice decentralization or security.

Why It Matters

- High gas fees (~\$50-200 during peak) exclude everyday users
- Bitcoin Lightning Network launched in 2018, but adoption remains low
- Ethereum's Dencun upgrade (March 2024) reduced L2 fees by 90% via EIP-4844

What We Need

- Understanding design constraints
- Mechanisms that inherit L1 security while increasing throughput 10-1000x
- Solutions that don't require users to trust new validator sets

The Cryptoeconomics Question

How do we optimize for scalability without breaking decentralization or security?

Today's lesson: How Layer 2 Scaling addresses this challenge

The Trilemma:

Can only optimize 2 of 3 properties:

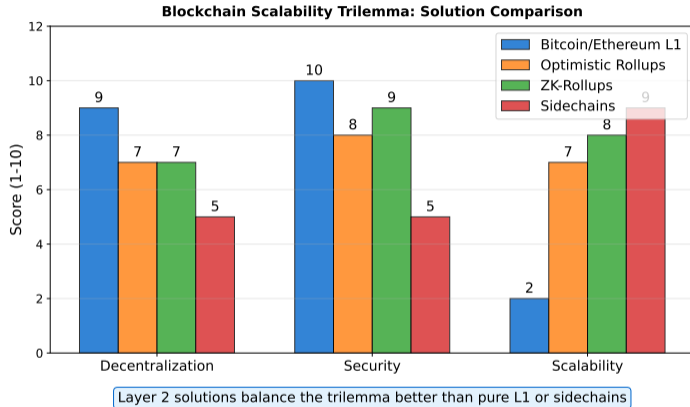
- **Decentralization:** Independent validators
- **Security:** Cost to attack network
- **Scalability:** TPS throughput

Current TPS:

- Bitcoin: ~7 TPS
- Ethereum: ~15 TPS
- Visa: ~65,000 TPS

Solution: Layer 2 moves transactions off-chain while inheriting L1 security

Trilemma Comparison by Solution



Rollups achieve better balance than L1 alone or sidechains

Layer 1 (L1)

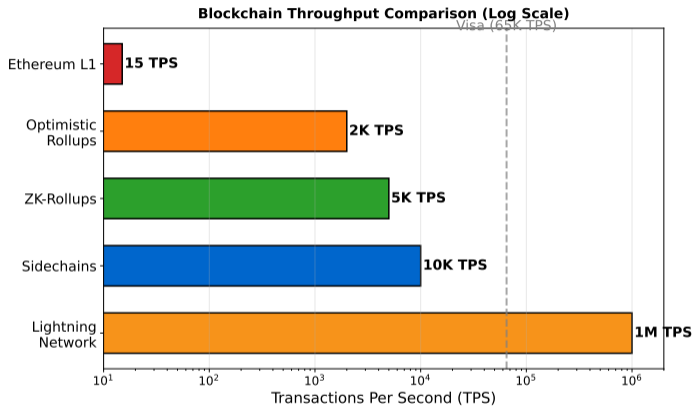
- Base blockchain protocol
- Full consensus for every transaction
- High security, low throughput
- Examples: Bitcoin, Ethereum

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

State Channels:

- P2P direct channels
- Ex: Lightning Network

Sidechains:

- Independent chain
- Two-way peg to L1

Rollups:

- Batch off-chain
- Post data on-chain

Optimistic: Fraud proofs
ZK: Validity proofs

Plasma:

- Child chains
- Merkle commits

Validium:

- Off-chain DA
- Validity proofs

Problem: Bitcoin's 7 TPS cannot support global payments

Solution: Bidirectional payment channels

Mechanism:

- 1 Open channel (on-chain funding)
- 2 Transact off-chain (update state)
- 3 Close channel (broadcast to L1)

Network Topology:

Channels form payment routing graph

Capacity:

- Millions of TPS possible
- Sub-second finality
- Minimal on-chain footprint

Core Idea:

Execute off-chain, post compressed data on-chain

Architecture:

- **Data Availability:** TX data on L1
- **Computation:** Off-chain sequencer
- **State Roots:** Merkle root to L1

Benefits:

- 100-1000x throughput gain
- Inherit L1 security
- Lower transaction costs

Two Variants:

Optimistic vs ZK (differ in validity proof)

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

Mechanism:

- Cryptographic validity proofs per batch
- SNARK/STARK: Prove without revealing
- L1 verifies proof (constant cost)
- Finality: \sim 10-30 min after proof

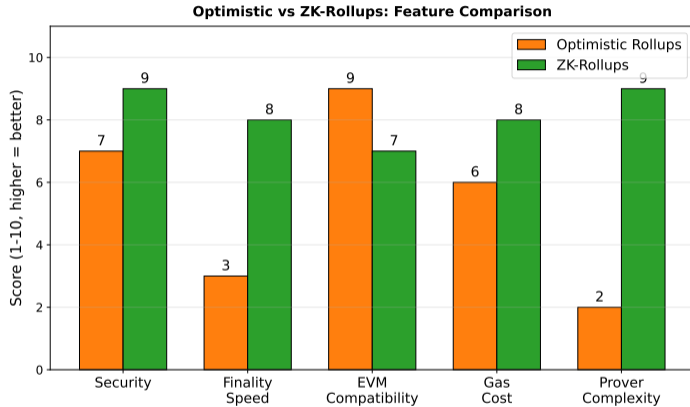
Advantages:

- Fast withdrawals (no challenge)
- Stronger security guarantees

Disadvantages:

- Complex crypto, higher prover costs
- EVM compatibility (improving)

Optimistic vs ZK-Rollups



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

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

Purpose: Transfer assets between L1/L2 or across chains

Lock-and-Mint Pattern:

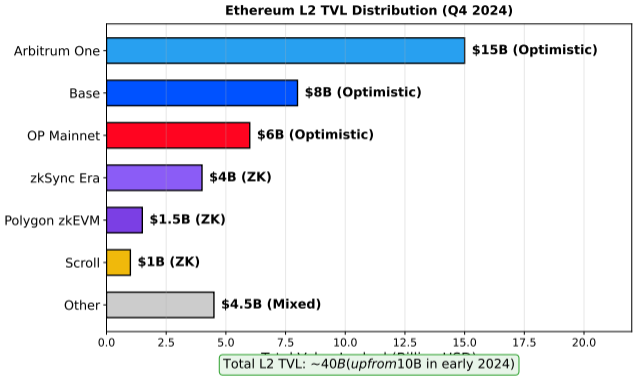
- 1 Lock assets on source chain
- 2 Mint wrapped tokens on dest
- 3 Burn to unlock original

Bridge Types:

- **Trusted:** Centralized (fast)
- **Federated:** Multi-sig ops
- **ZK-Verified:** Highest security

Risk: Major attack targets
(\$2B+ stolen 2022-2023)

L2 TVL Distribution



Arbitrum leads by TVL; optimistic rollups currently dominate

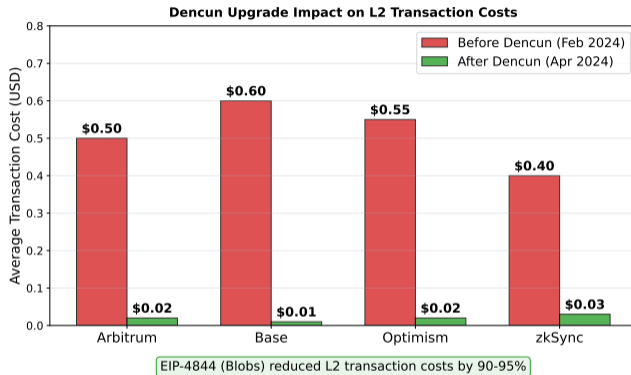
Dencun Upgrade (March 2024):

- EIP-4844 blob transactions
- L2 fees reduced by 90%+
- \$0.50-2.00 → \$0.01-0.05
- User migration accelerated

Key Trends:

- TVL: \$54B (205% YoY)
- L2 TX $\dot{\simeq}$ L1 daily volume
- App chains for specific use
- ZK maturity (zkSync, Scroll)

Dencun Impact on L2 Fees



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

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

Scaling:

- **Full Danksharding:** 100K+ TPS
- **zkEVM:** Full EVM equivalence
- **Layer 3:** App-specific rollups

Infrastructure:

- **Interoperability:** Cross-rollup comms
- **Sequencer Decentralization:** Remove SPOF
- **Shared Sequencing:** Multi-rollup infra

EOA Problems:

- Must hold ETH for gas
- Single key = single point of failure
- No batching (2 TX for approve+swap)
- Lost key = lost funds forever

ERC-4337 Solution:

- Programmable smart wallets
- Custom validation (multi-sig, recovery)
- Sponsored transactions
- Bundled ops (1 click)

No protocol changes required – works on existing Ethereum

Key Components

- **UserOperation**: Pseudo-transaction struct
- **Bundler**: Collects and submits UserOps
- **EntryPoint**: On-chain singleton contract
- **Smart Account**: User's wallet contract
- **Paymaster**: Pays gas on user's behalf

Transaction Flow

- 1 User signs UserOperation
- 2 Bundler collects UserOps
- 3 Bundler submits batch to EntryPoint
- 4 EntryPoint validates and executes
- 5 Paymaster (optional) covers gas

ERC-4337 achieves account abstraction without modifying Ethereum protocol

1. Gasless Transactions:

- DApp sponsors gas for users
- Pay gas in USDC/DAI

2. Social Recovery:

- Guardians can recover wallet
- No seed phrase SPOF

3. Session Keys:

- Limited time permissions
- Gaming: no constant signing

4. Batch Transactions:

- Approve+swap+stake in 1 click
- Better UX, lower gas

Account Abstraction Adoption (2024-2025)

Milestones:

- Mar 2023: ERC-4337 mainnet
- 2024: Major wallet integration
- Late 2024: 10M+ smart accounts
- 2025: Default on L2s

Leading Implementations:

- **Safe:** Multi-sig + modular
- **Coinbase:** Passkey-based
- **ZeroDev:** Developer SDK
- **Alchemy:** Bundler infra

Account abstraction is key to achieving Web2-like UX in crypto

The Original Problem

How do we scale without sacrificing security?

How Layer 2 Scaling Solves It

- **Optimistic Rollups:** Assume validity by default, use fraud proofs for disputes (7-day challenge period)
- **ZK-Rollups:** Prove correct execution cryptographically via SNARKs/STARKs (10-30 min finality)
- **State Channels:** Move repeated interactions off-chain, settle final state on L1 (Lightning Network)

Remaining Limitations

- **Bridge Risk:** \$2B+ stolen from cross-chain bridges (2022-2023)
- **Sequencer Centralization:** Most rollups use single sequencer (SPOF)
- **Withdrawal Delays:** Optimistic rollups require 7-day wait for L1 finality

Open Questions

- Will rollups become the dominant scaling paradigm, or will app-specific chains (L3s) fragment liquidity?
- Risk: Over-optimization for TPS at the expense of decentralization (sequencer monopolies)

Layer 2 Scaling solves throughput bottleneck but introduces new trust assumptions and operational complexity

L2 Solutions:

- **State Channels:** P2P, instant (Lightning)
- **Optimistic:** Fraud proofs, 7-day wait
- **ZK-Rollups:** Validity proofs, fast

Key Developments:

- **EIP-4844:** L2 fees ↓90%
- **ERC-4337:** Smart wallets UX
- **Future:** L3s, danksharding

L2 solutions scale blockchains while preserving decentralization and security

- 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 How does ERC-4337 solve the onboarding problem for new crypto users?

Quiz Questions (1–5)

Q1. What is the blockchain scalability trilemma?

- A) Trade-off between speed, cost, and privacy
- B) Trade-off between decentralization, security, and scalability
- C) Trade-off between throughput, latency, and data availability
- D) Trade-off between validators, miners, and users

Answer: B – The trilemma states you can only optimize 2 of 3 properties: decentralization, security, and scalability.

Q2. What is the approximate transaction throughput of Ethereum Layer 1?

- A) 7 TPS
- B) 15 TPS
- C) 65 TPS
- D) 1000 TPS

Answer: B – Ethereum L1 processes around 15 transactions per second, while Bitcoin does 7 TPS.

Q3. What is the primary purpose of Layer 2 solutions?

- A) Replace Layer 1 blockchains entirely
- B) Process transactions off-chain while inheriting L1 security
- C) Create new cryptocurrencies
- D) Increase the block size of Layer 1

Answer: B – L2s move computation off-chain but settle final state on L1, inheriting its security.

Q4. Which Layer 2 pattern is used by Bitcoin's Lightning Network?

- A) Rollups
- B) Sidechains
- C) State Channels
- D) Plasma

Answer: C – Lightning uses bidirectional payment channels for peer-to-peer transactions.

Q5. What is the key difference between Layer 2 rollups and sidechains?

- A) Rollups are faster than sidechains
- B) Sidechains are cheaper than rollups
- C) Rollups inherit L1 security; sidechains do not
- D) Sidechains use proof-of-stake; rollups use proof-of-work

Answer: C – Rollups post data to L1 and inherit its security, while sidechains have independent consensus.

Quiz Questions (6–10)

Q6. How do optimistic rollups verify transaction validity?

- A) Every transaction is verified immediately on L1
- B) Transactions are assumed valid unless challenged with a fraud proof
- C) Cryptographic proofs are generated for every batch
- D) A trusted third party validates all transactions

Answer: B – Optimistic rollups assume validity by default and allow anyone to submit fraud proofs during a challenge period.

Q7. What is the typical withdrawal delay for optimistic rollups?

- A) Instant
- B) 10-30 minutes
- C) 7 days
- D) 30 days

Answer: C – The 7-day challenge period allows time for fraud proofs before finalizing state.

Q8. What type of cryptographic proofs do ZK-Rollups use?

- A) Proof-of-Work
- B) Fraud proofs
- C) SNARK/STARK proofs
- D) Merkle proofs

Answer: C – ZK-Rollups use SNARK or STARK zero-knowledge proofs to verify correct execution.

Q9. What is the main advantage of ZK-Rollups over optimistic rollups?

- A) Lower transaction costs
- B) Better EVM compatibility
- C) Fast finality without challenge period (10-30 min)
- D) Simpler technology

Answer: C – ZK-Rollups achieve finality after proof verification (10-30 min), avoiding the 7-day wait.

Q10. Which Ethereum upgrade significantly reduced L2 transaction fees in March 2024?

- A) The Merge
- B) Shanghai upgrade
- C) Dencun upgrade (EIP-4844)
- D) Shapella

Answer: C – Dencun introduced blob transactions (EIP-4844), reducing L2 fees by 90%+.

Quiz Questions (11–15)

Q11. What was the approximate fee reduction after EIP-4844 implementation?

- A) 10-20% reduction B) 50% reduction C) 90%+ reduction D) No change

Answer: C – L2 fees dropped from \$0.50-2.00 to \$0.01-0.05, a 90%+ reduction.

Q12. Which L2 solution currently leads by Total Value Locked (TVL)?

- A) Optimism B) Arbitrum C) zkSync D) Polygon zkEVM

Answer: B – Arbitrum has the highest TVL among Ethereum Layer 2 solutions.

Q13. What is the primary security risk associated with cross-chain bridges?

- A) High gas fees
B) Slow transaction speed
C) Major attack target (\$2B+ stolen in 2022-2023)
D) Incompatibility with smart contracts

Answer: C – Bridges are vulnerable to attacks, with over \$2B stolen in recent years.

Q14. What is the “lock-and-mint” pattern used for?

- A) Creating new cryptocurrencies
B) Transferring assets between chains via bridges
C) Mining new blocks
D) Validating transactions

Answer: B – Assets are locked on source chain, wrapped tokens minted on destination, then burned to unlock.

Q15. Which trust model provides the highest security for bridges?

- A) Trusted (centralized custodian)
B) Federated (multi-sig operators)
C) ZK-Verified (cryptographic proofs)
D) All are equally secure

Answer: C – ZK-verified bridges use cryptographic proofs for the highest security level.

Quiz Questions (16–20)

Q16. What is the combined Layer 2 TVL as of late 2024?

- A) \$15B
- B) \$30B
- C) \$54B
- D) \$100B

Answer: C – Combined L2 TVL reached \$54B by Dec 2024 (205% YoY growth).

Q17. What is a Layer 3 (L3) solution?

- A) A faster version of Layer 1
- B) Application-specific rollups built on top of Layer 2
- C) A replacement for Layer 2
- D) A sidechain for Layer 1

Answer: B – L3s are specialized rollups built on L2s for specific applications.

Q18. What does “sequencer decentralization” aim to address?

- A) High transaction fees
- B) Slow transaction speed
- C) Single point of failure in L2 architecture
- D) EVM compatibility issues

Answer: C – Decentralizing sequencers removes the centralized bottleneck in current L2 designs.

Q19. What is the primary advantage of state channels like Lightning Network?

- A) Highest security
- B) Instant finality with millions of TPS
- C) Best for smart contracts
- D) Lowest setup cost

Answer: B – State channels enable instant finality and can handle millions of TPS for payments.

Q20. What future upgrade promises 100,000+ TPS through massive data availability?

- A) EIP-4844
- B) Full Danksharding
- C) The Merge
- D) zkEVM

Answer: B – Full Danksharding will dramatically increase data availability, enabling 100,000+ TPS.

Quiz Questions (21–24) – Account Abstraction

Q21. What standard defines Account Abstraction on Ethereum?

- A) ERC-20
- B) ERC-721
- C) ERC-4337
- D) EIP-1559

Answer: C – ERC-4337 enables smart contract wallets without protocol changes.

Q22. What component in ERC-4337 allows third parties to pay gas for users?

- A) Bundler
- B) EntryPoint
- C) Paymaster
- D) UserOperation

Answer: C – Paymasters sponsor gas fees, enabling gasless transactions for users.

Q23. Which is NOT a benefit of Account Abstraction?

- A) Social recovery of wallets
- B) Gasless transactions
- C) Faster block times on L1
- D) Batch transactions in single click

Answer: C – Account abstraction improves wallet UX, not L1 block production speed.

Q24. What role does the Bundler play in ERC-4337?

- A) Validates smart contracts
- B) Collects UserOperations and submits them to EntryPoint
- C) Stores user private keys
- D) Processes fraud proofs

Answer: B – Bundlers aggregate UserOps and submit batches to the EntryPoint contract.