Layer 2 Scaling Solutions for Blockchain Networks: An Analysis of Rollups, State Channels, Sidechains and Sharding

Azizgul Azizhussaini
Hemchandracharya North Gujarat University, Department of Computer Science

Abstract: ***Layer 2 scaling solutions have emerged as the primary approach to addressing blockchain scalability limitations while preserving security and decentralization. This paper presents a comprehensive comparative analysis of the four major categories of Layer 2 solutions: rollups (both optimistic and zero-knowledge), state channels, sidechains, and sharding. We examine the technical architectures, security models, performance characteristics, and trade-offs of each approach through synthesis of peer-reviewed research and empirical data. Our analysis reveals that rollups have emerged as the dominant scaling paradigm for Ethereum, with EIP-4844 reducing rollup costs by over 80%. ZK-rollups offer cryptographic security guarantees but face EVM compatibility challenges, while optimistic rollups provide full EVM equivalence at the cost of 7-day withdrawal periods. State channels excel for high-frequency bilateral transactions but lack generalpurpose applicability. Sidechains sacrifice L1 security inheritance for maximum throughput. We provide a decision framework for selecting appropriate solutions based on application requirements and discuss the convergent future of hybrid approaches combining multiple scaling techniques.***

Keywords: Layer 2 Scaling, Blockchain, Rollups, Zero Knowledge Proofs, State Channels, Sidechains, Sharding, Ethereum, Data Availability

I. SECURITY

The security model that best applies to many L2 solutions is cryptographic, meaning there's a public key system for consensus to be maintained at all times. Therefore, an entity is only trusted while it has not acted maliciously; should it do something wrong, either fraud proofs will punish it or it will be subsequently taken off the network. In contrast, centralized models do not trust transaction validation as secure, and thus, constant monitoring is needed. Therefore, the only way to increase throughput, in this case, is through immediate transactions like payment channel-like transactions without a definitive bridge to keep consensus in place over time.

Table 1 below highlights the security models that apply to the chosen L2 solutions and further discusses the concept of trust needed to better assess inherent assumptions. Generally, all L2 solutions get their security through L1 without a data availability (ZK-Rollups; Optimistic Rollups; state channels) or centralized model (state chains).

Table 1: Trust Assumptions by L2 Category

Solution	Trust Model	Security
ZK-Rollup	Cryptographic	Full L1
Optimistic Rollup	1-of-N honest	Full L1
State Channel	N-of-N online	Full L1
Sidechain	Separate validators	Independent
Validium	DAC committee	Partial L1

I.1. Optimistic Rollups

Optimistic Rollups operate under the assumption that transaction batches are valid without any initial scrutiny. They rely on fraud proof mechanisms that allow for challenge and eventual dispute resolution if a malicious actor attempts to act on an invalid transaction [4].

1.1.1. Architecture

The core components include:

1. Sequencer: Orders and batches L2 transactions
2. State Commitments: Merkle roots posted to L1
3. Challenge Period: 7-day window for fraud proofs
4. Fraud Proof System: Dispute resolution mechanism

1.1.2. Fraud Proofs

Optimism relies on *single-round fraud proofs*, where the entire disputed transaction is re-executed on L1.

This is easier, but more gas costly to challenge [8]. Arbitrum depends on *multi-round interactive fraud proofs*, where the invalid instruction is separated from others via bisection to determine just one thing wrong with the transaction. This saves gas on L1, but takes longer to settle [7].

Algorithm 1: Arbitrum Bisection Protocol

1. claim ← asserter's state commitment 2. steps ← number of execution steps
3. While steps >1:
   (a) mid ← steps/2
   (b) Asserter posts intermediate state at mid
   (c) Challenger selects disputed half
   (d) steps ← steps/2
4. Execute single instruction on L1
5. Verify against claimed state

1.1.3. Performance Metrics

- Arbitrum 4,500 TPS theoretical, 40,000 TPS by claim with Nitro [9]
- Optimism 2,000 TPS theoretically as capable
- Gas fee Arbitrum 0.051 Gwei average, Optimism 0.116 Gwei average (2024) [10]
- Block time Optimism 2 seconds fixed, Arbitrum variable

1.2. ZK-Rollups

ZK-Rollups rely upon zero-knowledge proofs that cryptographically authenticate transactions as valid instead of relying upon a challenge period for any fraud-proofs needed [5].

1.2.1. Proof Systems

There are two dominant proof systems
zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge): zkSync Era, Polygon zkEVM use this, which means:

- Requires trusted setup ceremony,
- Smaller proof sizes (~288 bytes) exists
- Not quantum resistant.

zk-STARKs (Zero-Knowledge Scalable Transparent Arguments of Knowledge):

- StarkNet (StarkWare) uses this, which means:
- No trusted setup necessary,
- Larger proof sizes (roughly 45-200 KB) exist,
- Quantum resistant, exists,
- Faster proof generation.

1.2.2. Comparison: zkSync vs StarkNet

Nethermind's empirical comparison exists between the two in [11]:

Table 2: ZK-Rollup Technical Comparison

Attribute	zkSync Era	StarkNet
Proof System	SNARK (Boojum)	STARK
EVM Compat.	99% (via Yul)	Cairo VM
Trusted Setup	Required	Not required
Quantum Res.	No	Yes
Proof Size	Small	Large
L1 Verify Cost	Lower	Higher
Batch Size	750-1000 tx	Variable

1.2.3. EVM Compatibility Solutions

ZK-Rollups are inherently challenged to achieve EVM equivalence due to ZK-unfriendly opcodes (i.e., hashing through Keccak-256). These include:

- Language-level: StarkNet implements its own Cairo programming language
- Bytecode-level: zkSync implements Solidity → Yul → zkEVM bytecode
- Transpilation: Warp (Nethermind) implements Solidity to Cairo
- Type-1 zkEVM: True equivalence (Taiko, under development)

1.3. Security Comparison

Security assurance properties of Rollups differ: Optimistic Rollups:

- Only rely upon honest verifier assumption of 1-of-N
- Subject to censorship in a challenge period due to L1 delays
- DoS could fail access to Fraud Proof operation
- ⇒ 7-day exit period for L1 security

ZK-Rollups:

- Cryptographic validity assurances
- No 1-of-N honest minority assumption exists
- Proof approval provides immediate finality
- However, if there are bugs in the circuit, security is at stake

II.STATE CHANNELS

State channels implement off-chain interactions that enable multiple transactions among designated parties with no contracts needed for on-chain each intermediate state [12].

II.1. Lightning Network

The Lightning Network (LN) is Bitcoin's native layer 2 operation, Hash Time-Locked Contracts (HTLCs) to allow multi-hop payments without trusted third parties [6].

2.1.1. Architecture

1. Funding Transaction: Initiates channel with collateral on-chain during production.
2. Commitment Transactions: Incrementally updates channel state off-chain.
3. HTLC routing: Reroutes payments across channel network.
4. Settlement: Closes channel with final balances reported.

2.1.2. Performance and Limitations

Guasoni et al. [13] assess LN from an economic perspective:

- Instant transaction finality (essentially)
- Fees lower than sub-satoshi for each routed payment.
- However, payment requires capital locked inside channels making liquidity non-existent.
- Payments fail due to routing (>capacity) or a lack of routes (each channel).
- Payment-induced balance probing accounts have privacy concerns.

Zabka et al. [14] assess LN from a centralizing perspective:

- Gini index increased by 15% over 2 years.
- Only a limited set of nodes route most transactions.
- A hub-and-spoke topology may be emerging.

2.2. Raiden Network

Raiden implements state channels on Ethereum with other ERC-20 transfers. The differences include:

- Arbitrary token transfers (beyond currency transfers) are supported.
- Matrix based message delivery.
- Pathfinding services to identify routing options.
- Lower penetration rates than Lightning Network.

2.3. State Channel Limitations

Miller et al. [15] identify the following fundamental limitations of state channels:

- Capital Inefficiency: Money is locked per channel.
- Online Participation: All parties must be online to detect fraud.
- Fixed Participants: You can't add additional participants later on.
- Application: Limited to payments and minor smart contracts.

III.SIDECHAINS

Sidechains operate distinct blockchains with bridges to Layer 1 separated by consensus mechanisms and their own operations. [16]

III.1. Polygon PoS

Polygon (formally Matic) operates as a sidechain with checkpoints every so often to Ethereum through Proof of Stake elements. [17].

3.1.1. Architecture

- Heimdall Layer: Confirms block, delivers checkpoints.
- Bor layer: Produces blocks via Tendermint-based consensus mechanism.
- Checkpoint mechanism: Delivers states every so often to Ethereum.
- Plasma Bridge: Asset transfer mechanism between POS and Ethereum.

3.1.2. Security Structure

Unlike Rollups, Polygon PoS security comes from its validator set:

- ~100 active validators (compared to Ethereum's 1,000,000+) in the validator pool.
- Staking MATIC token yields no sybil attacks enabled by other networks.
- Checkpoints only deliver a rollback on Ethereum for resolution purposes over time - gaps exist.
- Not a true layer 2 as it operates under its own assumptions of trust as well.

3.1.3. Performance

Polygon PoS boasts a massive level of transactions per second in testing:

- 7,000 TPS in simulation testing.
- Transactions less than $0.01 per transaction.
- Block time seconds – 2 seconds exact.
- EVM Compatible for Polygon operations are equal to those of Ethereum levels.

3.2. Security Trade-offs

Unlike Layer 1-Rollup structures that borrow Layer 1 security, sidechains give up certain versions of guarantees over performance:

Table 3: Sidechains vs Rollups Over Security

Property	Rollup	Sidechain
Source of Security	L1 consensus	Own validators
Security of Assets	L1 guarantees	Bridge-dependent
Data Availability	L1 or DAC	Sidechain nodes
Finality	L1 blocks	Sidechain blocks
Attack on 51%	L1 costs	Sidechain costs

IV.SHARDING: ETHEREUM DANKSHARDING

Sharding distributes blockchain state across several different chains (shards) that process transactions simultaneously. Ethereum's implementation transformed from execution sharding to data sharding which is optimal for rollups/integrated rollups with offloading data through additional chains and therefore less pressure on all decentralized nodes to create blocks at once [18].

IV.1. Proto-Danksharding (EIP-4844)

Implemented March 13, 2024, EIP-4844 implements blobcarrying transactions for future temporary data availability brought back to the Rollup Chain by these blobs. [19].

4.1.1. Technical Specifications

- Blob Size: 128 KB (4096 field elements × 32 bytes)
- Blobs per Block: Targeted 3, max 6
- Data Capacity: Average: 0.375 MB/slot
- Retention: ~18 days (4096 epochs)
- Commitment: KZG polynomial commitments

4.1.2. Impact on Rollup Economics

Park et al. have studied the impact of EIP-4844, empirically speaking:

Table 4: EIP-4844 Impact Metrics

Metric	Pre-4844	Post-4844
Arbitrum gas fee	$0.37	$0.012
Optimism gas fee	$0.32	$0.009
Cost per MiB	Baseline	-82%
Optimistic calldata	100%	-81%
Total data posted	Baseline	+100%

4.2. Full Danksharding

The full Danksharding specification builds upon ProtoDanksharding:

- 64 blobs per block (6 currently)
- Data Availability Sampling for light clients
- Proposer-Builder Separation
- Timeframe: 2-3 years
- Data Availability target: 1.3 MB/s

4.2.1. Data Availability Sampling

Data Availability Sampling allows light nodes to confirm data availability without needing to download entire blocks of data [21]:

1. Erasure code blob data (2D Reed-Solomon)
2. Random chunks are sampled by light nodes randomly/repeatedly.
3. Statistical guarantee—75% to indicate probability of having it with high success rate if it is all there.
4. Minimal bandwidth access for trustless confirmation.

V.DATA AVAILABILITY

Data availability is a crucial security property to ensure data is available so the state can be reconstructed, and fraud proofs can be generated [22].

5.1. The Data Availability Attack Vector

The rollup can imply a data availability attack vector: an operator can submit a valid state root without providing any data. Thus, it can withhold:

- Transaction details, therefore, cannot confirm the transaction,
- State can not be validated asynchronously,
- Fraud Proofs cannot be generated (Optimistic Rollups)
- User exit cannot occur (Plasma/Validiums)

5.2. DA Solutions Overview

We can structure potential solutions into a taxonomy of approaches: which each varying degrees of cost and security.

Table 5: Cost and Security Classification of DA Approaches

Method	Security	Cost
L1 Calldata	Highest	High
L1 Blobs (4844)	High	Medium
DA Committee	Medium	Low
External DA Layer	Variable	Lowest

5.3. External DA Layers

Celestia, EigenDA and Avail offer DA outside the Ethereum space. They all include:

- Consensus optimized for DA
- DA Sampling built-in
- L1 security at a cost, albeit decreased
- Validiums use DACs to attest the availability of DA.

VI.COMPARISON TABLE AND OVERVIEW

VI.1. Performance Comparison Across Solutions

Table 6 summarizes performance characteristics across solutions that represent comparative advantages by prioritizing different features.

Table 6: Comprehensive Performance Comparison

Solution	TPS	Finality	Withdrawal
Arbitrum	4,500	Minutes	7 days
Optimism	2,000	Minutes	7 days
zkSync Era	2,000+	Hours	Minutes
StarkNet	1,000+	Hours	Minutes
Lightning	Unlimited	Instant	Channel close
Polygon PoS	7,000	Seconds	Hours

VI.2. Security Guarantees

Security guarantees are strong and shift drastically for different systems.

Strongest Security (Cryptographic)

- ZK-Rollups–mathematical proofs of validity with zero knowledge–require no trust beyond logical cryptographic assumptions. Therefore, circuit bugs are the only attack vector.

Strong Security (Economic)

- Optimistic Rollups–the truth will be verified by an honest validator needed only one out of many to dispute the truth; fraud proofs will take time, but justice will prevail. Security concerns take place in the challenge period, where censorship can happen.

Moderate Security (Consensus)

- Moderately secured because they require user diligence– State Channels require being online; Sidechains operate outside of the L1 domain with their validator economics; Validiums with DACs require M-of-N committee to approve intent.

6.3. Cost Considerations

Since EIP-4844, the price for transaction cost predictions will favor various approaches:

- For $0.01-0.10 transactions on L2, they'll be worth it to avoid $1-10 on L1 (optional) based on context and congestion.
- ZK Proof generation may be high but is amortized and paid in batch.
- Sequencers are finding more revenue generation models but turning to decentralization as the solution.

VII.DECISION MODEL BASED ON THESE COMPARISONS ABOVE

7.1. Use Case Mapping

High Value DeFi / Exchanges

- ZK-Rollups
- Rationale: Security essential, finality valued–fast time for finality.
- Examples: dYdX (StarkEx), Loopring–strong emphasis on spot trading.

General Purposes/Smart Contracts

- Optimistic Rollups
- Rationale: Full EVM Compatibility; More established rolling up extensive DeFi ecosystems.
- Examples: Uniswap (Arbitrum), Synthetix (Optimism). High Frequency Small Payments
- State Channels
- Rationale: Near zero costs and instant finality in close bilateral transactions.
- Examples: Lightning payments through payment channels established between parties.

Gaming / Heavy Processing

- Sidechains or Validiums
- Rationale: Volume throughput means security is secondary potentially.
- Examples: Immutable X, Ronin for gameplay.

7.2. Selection Requirements

1. Reliability/Need security requirement? Critical assets? If yes→ZK-Rollup.
2. Need immediacy for withdrawal latency? If yes→ZK-Rollup.
3. EVM Compatibility? If yes→Optimistic Rollup.
4. Transaction volume? If very high→Validiums/Sidechains(throughput)
5. Transaction cost sensitivity? Micropayments→State Channels.

VIII.FUTURE PLANS

8.1. Technical Roadmap for Existing Systems/Proposed Improvements/Adjustment Needs:

- Full Danksharding: 64 blobs/block–DAS implementation.
- Type-1 zkEVM–and full equivalence for ZK-Rollups.
- Decentralized Sequencing–shared sequencing, based rollups where validiums can control.
- Cross-Rollup Interoperability–shared bridges and atomic composability.

8.2. Research Problems Facing These Systems:

- Proving polynomial operations in EVM proving/reducing in ZK circuits must eliminate valid sub-steps.
- Understanding MEV when using an L2 sequencer; essentially not supposed to happen but documented in note time opportunities.
- DAC security must be formalized across layers.
- Hybrid rollup designs must be achieved for OR/ZK approaches.

IX. SUMMARY

As Layer 2 Scaling solutions have come a long way–through the roadmap supporting rollups as the true future of EVM as we know it Thus–conclusions we can draw from this comparative analysis are relative to existing needs for DeFi protocols recently discovered.

1. ZK-Rollups have certain, valid edges of Security boasting cryptographic proofs substantiating their validity but suffering from EVM Compatibility and Proof generation overhead.
2. Optimistic rollups have the best EVM Compatibility and ease of implementation but take a security risk with 7-day withdrawal periods for any practical use case.
3. State Channels are great options for high-frequency bilateral transactions but fail to scale for general-purpose smart contracting fulfillment.
4. Sidechains sacrifice security inheritances per the proximity of L1 benefits for maximum throughput at minuscule cost.
5. EIP-4844 is a major milestone that reduces rollup-level data collection by 82% while creating a Danksharding infrastructure for these approaches to work fully later down the line–1 year planned; many unknowns proposed to make them viable later down the road.

These conclusions ultimately emphasize that finding the appropriate solution will depend on application needs. As support increases for further improvements down the line in the coming decade or so, it's clear that systems will trend toward hybrids combining ZK proof validity with optimistic execution patterns while advances on other fronts take place to support decentralized sequencing as well as cross-rollup composability.

REFERENCES

[1] A. Hafid, A. S. Hafid, and M. Samih, "Scaling blockchains: A comprehensive survey," *IEEE Access*, vol. 8, pp. 125244–125262, 2020.

[2] Q. Zhou et al., "Solutions to scalability of blockchain: A survey," *IEEE Access*, vol. 8, pp. 16440–16455, 2020.

[3] S. Reno and K. Roy, "Navigating the blockchain trilemma: A review of recent advances," *Computers, Materials & Continua*, vol. 84, no. 2, pp. 2061–2119, 2025.

[4] C. Sguanci, R. Spatafora, and A. M. Vergani, "Layer 2 blockchain scaling: A survey," *arXiv preprint arXiv:2107.10881*, 2021.

[5] L. T. Thibault, T. Sarry, and A. S. Hafid, "Blockchain scaling using rollups: A comprehensive survey," *IEEE Access*, vol. 10, pp. 93039–93054, 2022.

[6] J. Poon and T. Dryja, "The bitcoin lightning network: Scalable off-chain instant payments," 2016.

[7] H. Kalodner et al., "Arbitrum: Scalable, private smart contracts," in *Proc. 27th USENIX Security Symposium*, 2018.

[8] TokenInsight, "Optimism vs. Arbitrum: A complete comparison," 2022.

[9] Guardarian, "Arbitrum vs Optimism: A comprehensive comparison," 2024.

[10] Across Protocol, "Optimism vs Arbitrum: A complete L2 comparison guide," 2024.

[11] E. Barbieri, "Starknet and zkSync: A comparative analysis," *Nethermind Research*, 2024.

[12] L. D. Negka and G. P. Spathoulas, "Blockchain state channels: A state of the art," *IEEE Access*, vol. 9, pp. 160277–160298, 2021.

[13] P. Guasoni, G. Huberman, and C. Shikhelman, "Lightning network economics: Channels," *Management Science*, vol. 70, no. 6, pp. 3827–3840, 2024.

[14] P. Zabka et al., "A centrality analysis of the Lightning Network," *Telecommunications Policy*, vol. 47, no. 9, 2023.

[15] A. Miller et al., "Sprites and state channels: Payment networks that go faster than lightning," in *Financial Cryptography and Data Security*, 2019.

[16] A. Singh et al., "Sidechain technologies in blockchain networks: An examination and state-of-the-art review," *J. Network and Computer Applications*, vol. 149, 2020.

[17] Polygon Labs, "Polygon 2.0: Protocol vision and architecture," 2023.

[18] J. Bonneau et al., "Data availability sampling and danksharding: An overview," *a16z crypto*, 2023.

[19] V. Buterin et al., "EIP-4844: Shard blob transactions," *Ethereum Improvement Proposals*, 2022.

[20] S. Park et al., "Impact of EIP-4844 on Ethereum: Consensus security, Ethereum usage, rollup transaction dynamics, and blob gas fee markets," in *Proc. ACM CCS*, 2024.

[21] Celestia, "The data availability problem," 2024.

[22] E. Damiano et al., "A survey on data availability in layer 2 blockchain rollups," *Future Internet*, vol. 16, no. 9, 2024.

[23] S. Parashar et al., "Understanding blockchain trilemma, causes and solutions," in *Proc. IEEE ICCCNT*, 2024.

[24] K. M. Shafin and S. Reno, "Breaking the blockchain trilemma: A comprehensive consensus mechanism," *IET Software*, 2024.

[25] Messari, "Optimism vs Arbitrum," 2024.

[26] Gate.io Research, "Starknet comprehensive report," 2024.

[27] C. Ndolo and F. Tschorsch, "On the (not so) surprising impact of multi-path payments on performance and privacy in the Lightning Network," in *ESORICS*, 2024.

[28] ACM CCS, "Payout races and congested channels: A formal analysis of security in the Lightning Network," 2024.

[29] BitGo, "Danksharding: Scaling Ethereum," 2024. [30] Ethereum Foundation, "Data availability," *ethereum.org*, 2024.

[31] Alchemy, "What is the data availability layer?" 2024.

[32] Halborn, "How ZKPs make ZK-rollups superior to optimistic rollups," 2024.

[33] StarkWare, "ZK rollups vs. optimistic rollups: How do they compare?" 2024.

[34] CoinGecko, "What is data availability in blockchains?" 2024.

[35] Hacken, "Impact of EIP-4844 on Ethereum: What you need to know," 2024.

[36] G. D. Monte, D. Pennino, and M. Pizzonia, "Scaling blockchains without giving up decentralization and security," in *Proc. CryBlock Workshop*, 2020.

[37] IEEE, "Investigating Layer-2 scalability solutions for blockchain applications," in *Proc. IEEE ICBC*, 2024.

[38] SpringerLink, "A survey on Layer 2 solutions to achieve scalability in blockchain," 2022.

[39] IEEE COMST, "A survey on blockchain scalability: From hardware to layer-two protocols," 2024.