Optimistic vs ZK Rollups

Two ways to scale Ethereum — one assumes honesty and checks for fraud, the other proves correctness before it asks for trust.

Alain AI Lab Research · Published July 3, 2026 · 9 min read

AT A GLANCE

WHAT THEY ARE **Ethereum layer-2 rollups**	SHARED TRAIT **Batch transactions, post data to L1**	OPTIMISTIC **Assume valid, fraud proofs**
ZK **Validity proofs, no wait**	WITHDRAWAL **~7 days vs near-instant**	LONG-TERM THESIS **ZK favored as tech matures**

01 — THE FOUNDATION

What a Rollup Actually Is

A rollup is a layer-2 scaling solution — a separate network that sits on top of a base blockchain, in this case Ethereum, to process transactions more cheaply and quickly. Instead of executing every transaction directly on Ethereum's main chain, known as layer-1 or L1, a rollup carries out the work off to the side and then posts the results, along with the underlying transaction data, back down to L1. Because that data lands on Ethereum, the rollup inherits much of Ethereum's security rather than having to build its own from scratch.

The reason rollups exist at all comes down to cost and congestion. When too many people compete for space in Ethereum's limited blocks, transaction fees spike — the dynamic we unpack in our explainer on why gas fees get so high. Rollups relieve that pressure by doing the heavy computation elsewhere and posting only a compressed summary to the expensive base layer. This lets hundreds or thousands of transactions share the cost of a single

footprint on Ethereum. The two dominant families of rollup — optimistic and zero-knowledge (ZK) — agree completely on this goal. Where they part ways is on a single deep question: how does the rest of the world know the rollup did its work honestly?

02 — COMMON GROUND

The Idea They Both Share

Before the differences, it is worth being precise about what optimistic and ZK rollups have in common, because it is more than people assume. Both take many individual transactions and bundle — or "roll up" — them into a single batch. Both compress that batch and publish the essential data to Ethereum so that anyone can, in principle, reconstruct the rollup's state. And both ultimately lean on Ethereum's base-layer security, the same proof-of-stake security that underpins the network we describe in what is Ethereum staking. Posting data to L1 is what makes something a genuine rollup rather than a looser sidechain.

That shared reliance on posting data to Ethereum was made dramatically cheaper by a 2024 upgrade. The EIP-4844 change, nicknamed proto-danksharding, introduced "blobs" — a dedicated, lower-cost lane of temporary data space built specifically for rollups. Rolled out with Ethereum's Dencun upgrade in early 2024, it sharply reduced the single biggest recurring expense rollups face: paying to publish their data on L1. Both rollup types benefited, and the cost of using layer-2 networks fell markedly afterward. The distinction that remains, then, is not about batching or data — it is entirely about the proof.

03 — TRUST, THEN VERIFY

How Optimistic Rollups Work

Optimistic rollups earn their name from a simple stance: they *assume* every batch of transactions is valid by default. The rollup posts its new state to Ethereum and, optimistically, expects that no one cheated. Nothing is proven upfront. Instead, the design relies on *fraud proofs* — a mechanism by which any honest observer who spots an invalid state transition can raise a challenge and mathematically demonstrate the fraud to Ethereum, which then rejects the bad batch and penalizes the party that submitted it.

For this to be safe, someone has to be watching. The security rests on what is called a "one-of-N honest" assumption: as long as at least one honest participant is monitoring and willing to submit a fraud proof, cheating is caught. To give challengers time to act, optimistic rollups impose a challenge window — typically around seven days — before a withdrawal back to Ethereum becomes final and trustless. That waiting period is the price of the

optimistic approach. Users who want out sooner can use third-party "fast bridge" services that front the funds for a fee, but doing so reintroduces a measure of counterparty trust that the native seven-day path avoids.

04 — PROVE, THEN TRUST

How ZK Rollups Work

Zero-knowledge rollups invert the logic. Rather than assuming honesty and watching for fraud, they prove correctness upfront. Each batch is accompanied by a *validity proof* — a compact cryptographic certificate, built with technology such as ZK-SNARKs or ZK-STARKs, that mathematically demonstrates the batch was computed correctly. Ethereum verifies that proof when the batch is posted. If the proof checks out, the state is valid, full stop; if it does not, the batch is simply rejected. There is nothing to challenge and nobody who needs to be watching.

Because validity is established immediately, ZK rollups need no seven-day challenge window. Withdrawals back to Ethereum can be far faster and remain fully trustless, bounded mainly by how quickly proofs are generated and posted rather than by an arbitrary waiting period. One point deserves emphasis, because the name misleads so many people: in most ZK rollups, "zero-knowledge" is used for *succinctness* — proving a large computation is correct in a tiny, quick-to-verify certificate — not for user privacy. The great majority of ZK rollups are fully transparent networks, not anonymity systems. The property being exploited is efficient, verifiable proof, not secrecy.

> The cleanest way to remember the split: an optimistic rollup says "trust me unless someone proves I'm lying," while a ZK rollup says "here is the proof I told the truth — check it yourself." Everything else follows from that one difference.

05 — SIDE BY SIDE

The Trade-offs That Matter

The two designs make opposite bets, and each bet has consequences. On **trust**, optimistic rollups depend on an economic, game-theoretic guarantee — the honest watcher — while ZK rollups depend on cryptography that needs no watcher at all. On **withdrawals and finality**, optimistic rollups offer quick soft confirmation on layer-2 but delay true, final settlement on Ethereum until the challenge window closes; ZK rollups reach hard finality as soon as their proof is verified. On **cost**, the burden shifts location: ZK rollups pay heavily to

generate their validity proofs, a computationally intensive task, whereas optimistic rollups compute cheaply but absorb the latency and capital-lockup cost of the waiting period.

The historically decisive trade-off, though, has been **compatibility**. Optimistic rollups reached mature compatibility with the Ethereum Virtual Machine — the environment that runs Ethereum smart contracts — earlier and more easily, because they did not need to prove general-purpose execution cryptographically. ZK rollups had to build "zkEVMs," systems that can generate validity proofs for arbitrary EVM code, which turned out to be a hard engineering problem. That gap gave optimistic rollups a real head start in attracting developers and applications. It has been narrowing steadily as zkEVM technology and proving performance improve, but it explains much of the landscape as it stands today.

06 — THE FIELD

Who Is Building What

On the optimistic side sit the two largest layer-2 networks by activity. Arbitrum, built by Offchain Labs, and OP Mainnet — the flagship chain of Optimism — have anchored the category. Optimism's open-source "OP Stack" framework has been especially influential: Coinbase's rapidly-growing Base network is built on it, and the stack now underpins a whole family of interoperable chains sometimes branded a "superchain." Arbitrum offers a parallel framework, Orbit, for launching additional chains atop its technology. This proliferation of rollups and rollups-on-rollups has been one of the defining infrastructure trends of recent years, a theme running through our Ethereum thesis on restaking and L2s.

On the ZK side, the roster is deep and technically varied. zkSync Era, from Matter Labs, and StarkNet, from StarkWare — which uses STARK proofs and its own Cairo programming language — are among the longest-running. Polygon zkEVM, Scroll, and Linea, the last built by ConsenSys, round out a competitive set of zkEVMs, several with their own tokens. Through 2023 and 2024, optimistic rollups generally held higher total value locked and user activity than their ZK counterparts, largely on the strength of that earlier compatibility advantage — but ZK adoption has been climbing as the technology matures.

07 — THE SHARED FINE PRINT

Risks Both Designs Carry

Whichever proof mechanism a rollup uses, it shares a set of risks that have little to do with fraud proofs or validity proofs. The most important concerns the *sequencer* — the entity that orders transactions and assembles them into batches. Many rollups, both optimistic and ZK,

launched with a single centralized sequencer. Such a sequencer cannot generally steal funds, because Ethereum still enforces the validity of the final state, but it can censor or reorder transactions, extract value from their ordering, and represent a single point of failure. Decentralizing sequencers, and adding "escape hatches" that let users exit even if the operator misbehaves, has been an ongoing, phased effort across the industry.

To track how far along each network is, the community uses a "stages" framework — associated with Ethereum co-founder Vitalik Buterin and publicly monitored by independent analysts — that grades rollups from Stage 0, with heavy training wheels and upgradeable admin keys, up to fuller decentralization. It is a reminder that many rollups are still maturing systems, not finished ones. Also worth distinguishing are adjacent designs that are not pure rollups: a "validium" uses validity proofs but keeps its data off-chain, trading some of Ethereum's data-availability security for lower cost. That is a different risk profile from a true rollup, even when the underlying proof technology looks similar.

08 — THE LONG GAME

Which Approach Wins?

It is tempting to want a single winner, but the honest answer is that the two designs have been converging on the same destination from different directions. Optimistic rollups won the early practical race by being easier to build and easier for developers to adopt, and they still carry enormous activity. ZK rollups arrived with the theoretically stronger model — cryptographic certainty and fast, trustless exits — but had to overcome hard engineering before they could compete on general-purpose applications.

The prevailing view across much of the ecosystem, voiced by Vitalik Buterin among others, is that validity proofs represent the long-term end state: as proving costs keep falling and zkEVMs keep maturing, the reasons to prefer the optimistic model may gradually erode. That is a well-supported thesis, not a settled fact, and reasonable builders still disagree about the timeline. For now, both approaches coexist, both post their data to Ethereum, and both compete to make using the network cheaper without giving up its security. The optimistic path trusts first and verifies on challenge; the ZK path verifies first and asks for trust only after. Which philosophy you find more convincing may say as much about your appetite for risk as about the technology itself.

“The simple believeth every word: but the prudent man looketh well to his going.”

PROVERBS 14:15

METHODOLOGY & SOURCES

This report synthesizes public documentation from major layer-2 networks, Ethereum research including the 2020 rollup-centric roadmap and the EIP-4844 (proto-danksharding) specification shipped in the Dencun upgrade, and independent analyses of optimistic and zero-knowledge rollup architecture. It was prepared with a multi-agent verification process in which claims were independently checked and cross-referenced.

Figures relating to total value locked, transaction counts, fees, and withdrawal windows are directional and change continually; the roughly seven-day optimistic challenge window is a configured parameter, not a fixed law, and readers should consult live sources for current values. The expectation that ZK rollups become the long-term end state is presented as the prevailing industry thesis rather than an established outcome. Nothing here is investment advice; layer-2 networks vary widely in maturity, decentralization, and risk, and should be evaluated individually.

Alain AI Lab — independent crypto & AI research.
intelligencecrypto.org · This document is for educational purposes only and is not financial advice.