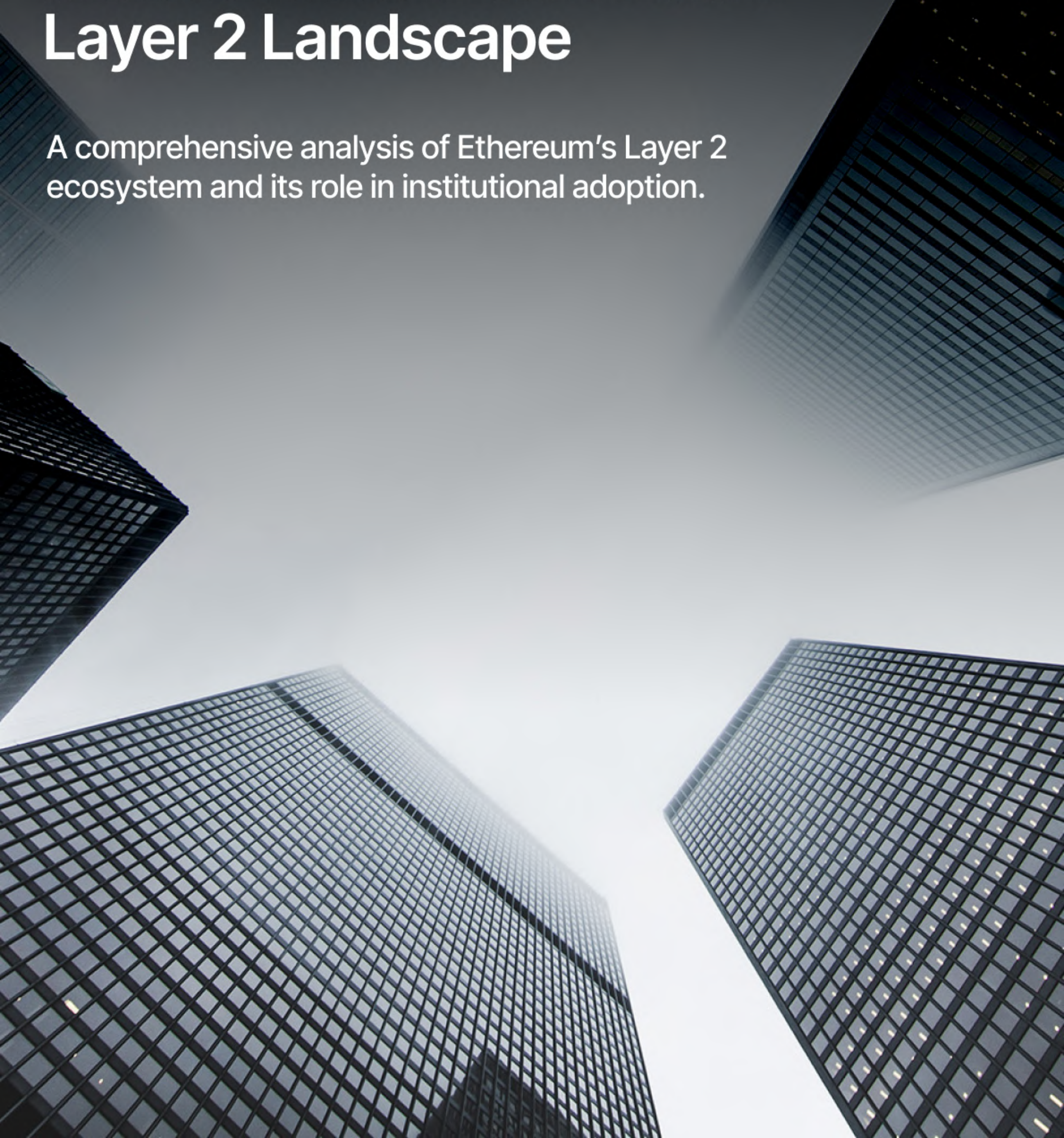
ETHEREALIZE NETHERMIND L2BEAT

The Future of Financial Infrastructure: Ethereum's Layer 2 Landscape

A comprehensive analysis of Ethereum's Layer 2 ecosystem and its role in institutional adoption.



Introduction

The global economy is undergoing a profound shift: a move onto blockchain rails that will propel the financial system into the 21st century. Blockchains have evolved from proof-of-concept platforms into production systems that move trillions of dollars a year, with the vast majority of that volume happening on Ethereum. This report analyzes how that shift will continue, specifically with the rise of Ethereum's Layer 2 (L2) ecosystem.

1

L2 networks are where scalability and customization converge to make blockchain adoption practical for high-volume financial applications. These networks extend Ethereum's security guarantees while offering institutions new features to meet their requirements, such as orders of magnitude more throughput than Ethereum's Layer 1 (L1) mainnet, custom execution rules, cheap and scalable privacy, or enhanced regulatory/compliance infrastructure.

2

About this Report: We begin by grounding the discussion in Ethereum itself before explaining what L2s are, how they work, and why they matter. We then examine how these technologies address enterprise needs such as high throughput, ownership, privacy, compliance, and cost-efficiency. Finally, we outline best practices for adoption, from operating models to infrastructure selection and deployment. The goal is simple: to equip institutions with the clarity and confidence to move from pilots to full implementations, and to show how Ethereum and its L2s will serve as the foundation for the next generation of financial markets and the global economy.

Executive Summary

The global financial system is undergoing a fundamental infrastructure upgrade as blockchains evolve from experimental platforms into production systems moving trillions of dollars annually. Ethereum, together with its L2 ecosystem, has emerged as the foundation for this transformation.

Why Now?

Market maturity: Stablecoins settled approximately $27T last year, and leading firms (e.g., JPMorgan, BlackRock, Franklin Templeton, Société Générale) are already building on Ethereum infrastructure.

Regulatory clarity: Frameworks such as MiCA (in the EU) and the U.S. GENIUS and CLARITY Acts are reducing uncertainty and enabling compliant deployments.

Standards formation: The standardization of tokenized securities and onchain identity is accelerating. Early adopters play a critical role in shaping these protocols, allowing them to accrue compounding network value ahead of mass adoption.

The Strategic Advantages of Ethereum L2s

Ownership & control: Deploy a custom L2 to dictate specific governance and access standards, all while retaining the settlement security and liquidity advantages of the Ethereum mainnet.

Privacy and confidentiality: Zero-knowledge proofs enable verifiable compliance without exposing sensitive details; regulators can obtain evidence of required checks being performed while commercial data stays confidential.

Economic efficiency: Transaction costs that are orders of magnitude lower, combined with high throughput, make unit economics competitive with legacy rails.

Compliance architecture: Identity credentials and programmable controls move compliance from after-the-fact monitoring to mathematically enforceable, pre-trade validation at the protocol level.

Customization with interoperability: L2s can be tailored to specific use cases with custom execution rules, privacy settings, and access controls, without isolating liquidity, all while remaining composable with the broader Ethereum ecosystem.

Adoption Paths

Public vs. private L2s: While public L2s prioritize open access and broad distribution, private and permissioned alternatives offer enhanced oversight and alignment with regulatory frameworks. Both models retain the settlement assurance and capital efficiency of the Ethereum mainnet.

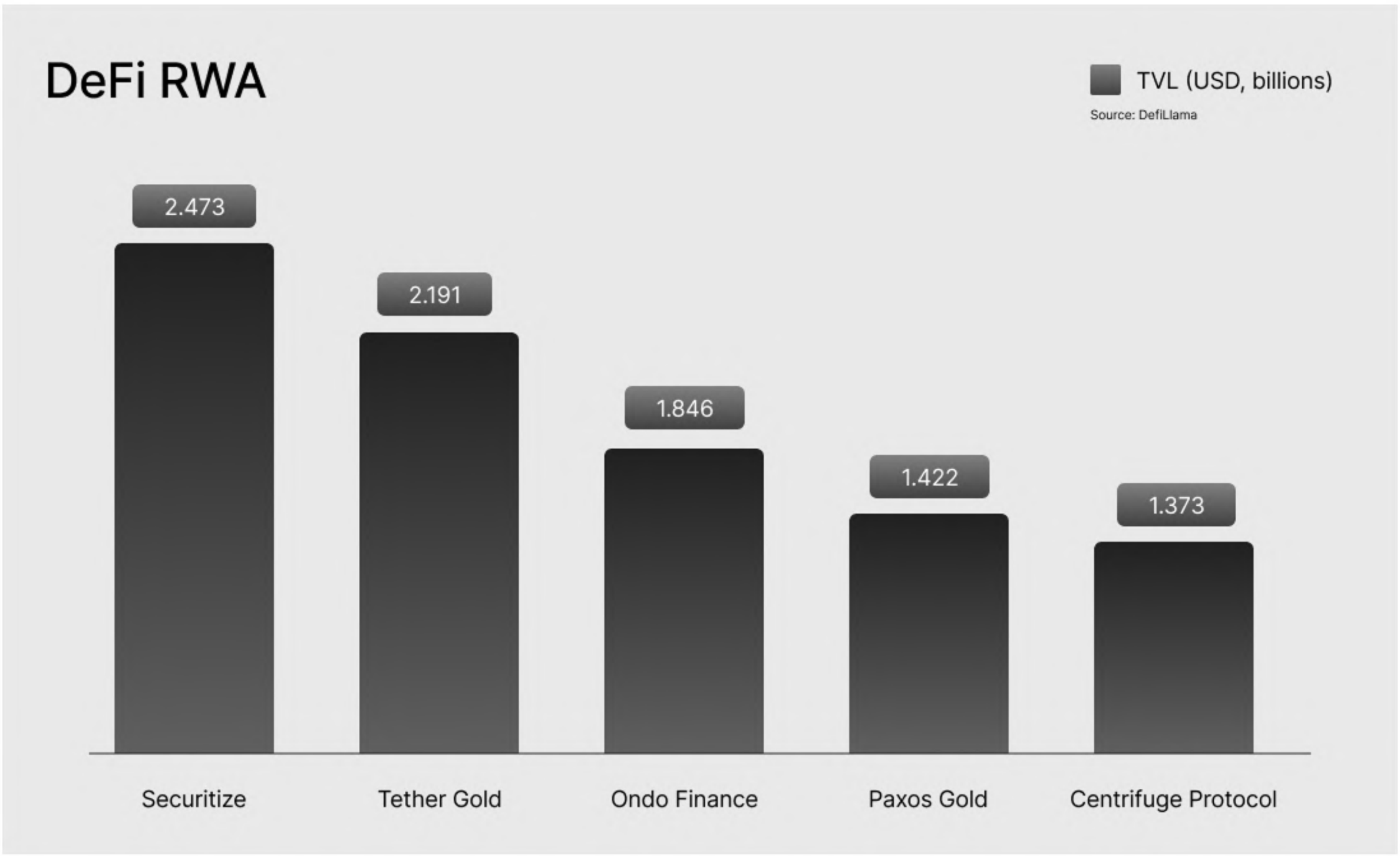
Selection criteria: Evaluate market fit and positioning, throughput requirements, compliance architecture, operational accountability, integration readiness with existing systems, and long-term strategic flexibility when deciding on whether or not to deploy an L2.

Use L1 where it counts: Canonical records and high-value settlement are typically kept on Ethereum mainnet; while L2s are used for scalable day-to-day operations.

Ethereum as the Foundation for Institutional Finance

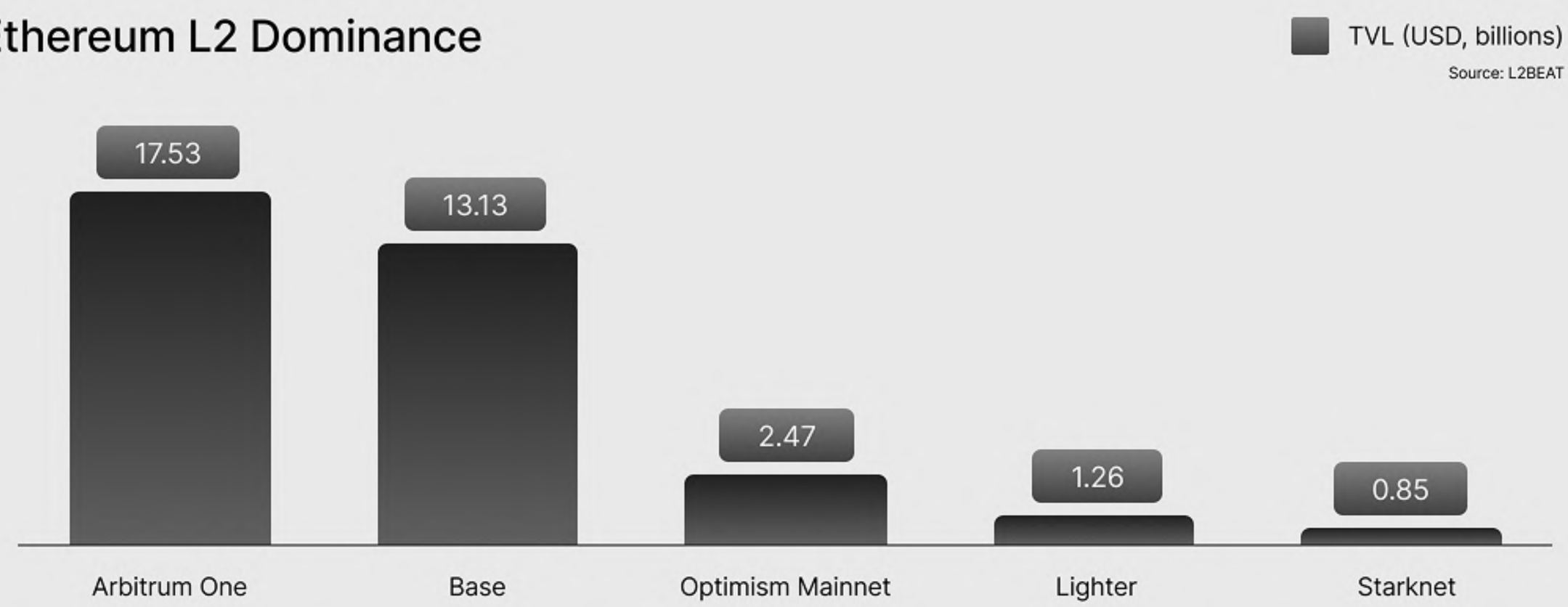
Ethereum is the foundational blockchain for institutional finance. It combines unmatched security, reliability, liquidity, neutrality, and ecosystem depth that no other chain comes close to. Since launching in 2015, Ethereum has operated with zero downtime, processing tens of trillions of dollars in stablecoin and crypto token value, all while continuously upgrading its core protocol without disruption.

This stability, combined with enterprise-ready tooling, a globally decentralized validator base, and a developer community larger than all its competitors combined, has created a network effect flywheel that makes Ethereum the default choice for institutions. It is where stablecoins reside, where tokenized assets are settled, and where financial innovation happens first. Firms such as J. P. Morgan and BlackRock (among countless others) are already building on Ethereum.

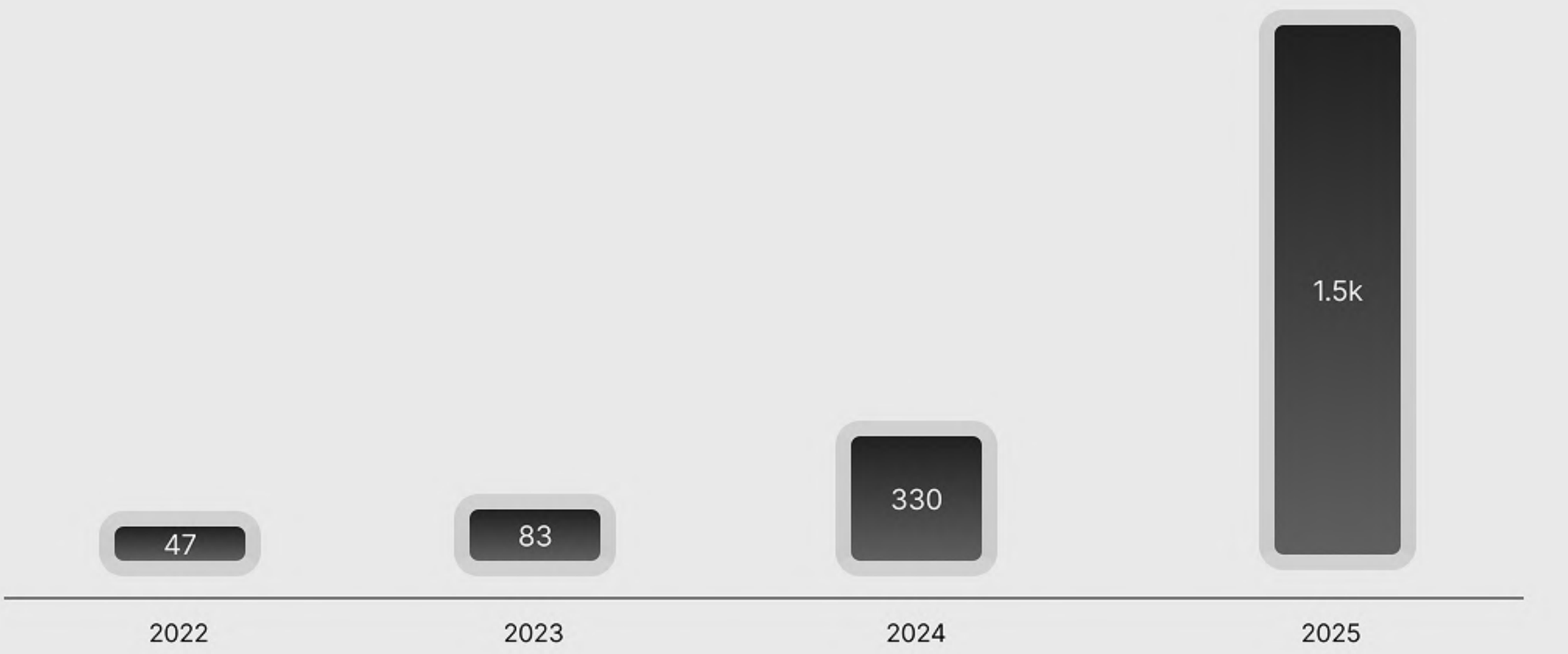


However, Ethereum's strengths are not limited to its base layer. The network's modular architecture enables scaling up activity without compromising security or neutrality. Ethereum's design allows Layer 2 solutions to inherit the trust of Ethereum while offering flexibility and higher performance. In other words, an institution can establish Ethereum-grade security as a foundation, then add an L2 on top as a customized environment for their specific needs, and be able to interoperate with other L2s as well. The case for Ethereum, therefore, extends beyond the main blockchain itself, and goes on to include Layer 2 infrastructure as a toolkit with which enterprises can innovate with confidence.

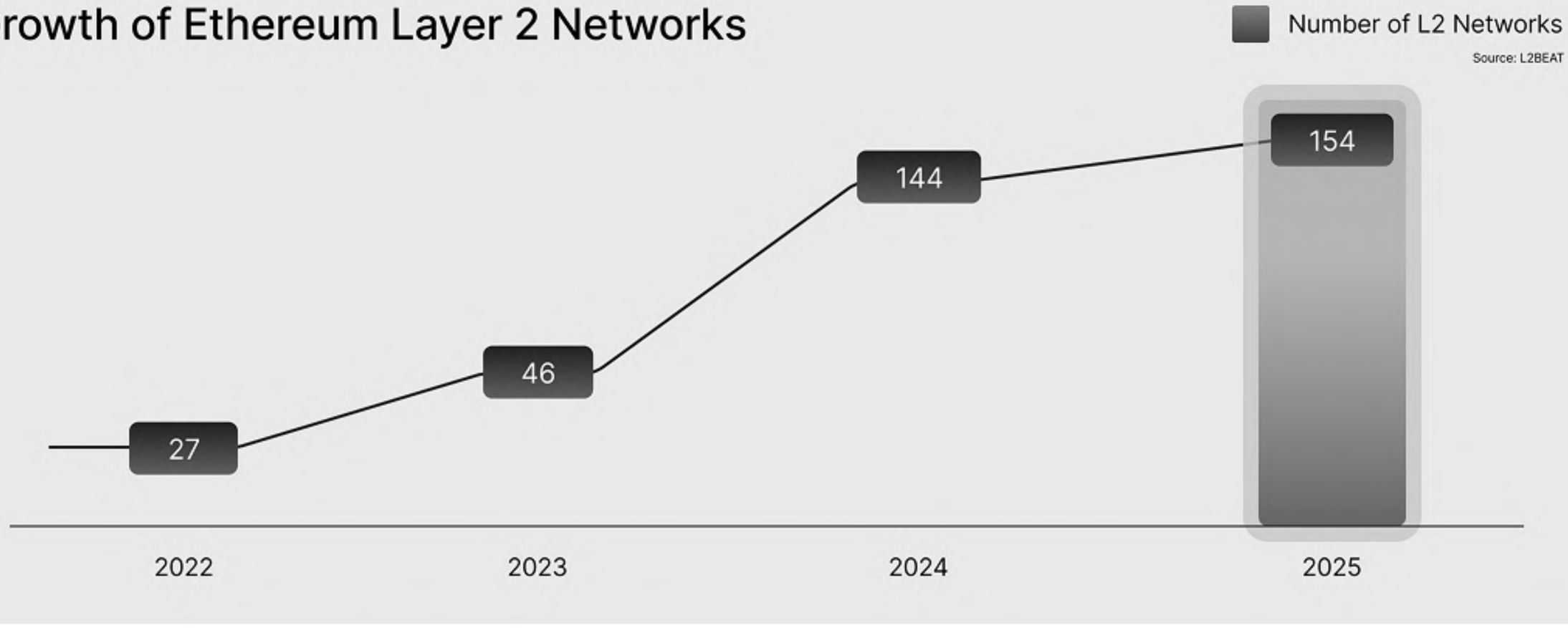
Ethereum L2 Dominance



Ethereum Ecosystem Throughput (TPS) Growth



Growth of Ethereum Layer 2 Networks



Why It's Time to Act Now

Timing defines outcomes in every wave of innovation. The firms that embraced the internet in the 1990s became today's market leaders; those that hesitated were often forced to play catch-up. We're at a similar inflection point with blockchain, except this shift is moving faster, with higher stakes, and far less room for late entry.

The numbers are making it clear. Stablecoins settled more than **$27 trillion** last year, a figure greater than Visa's annual payments volume. J.P. Morgan alone moves over **$2 billion** a day on Ethereum-based rails. What was once "experimental crypto" is becoming production-ready infrastructure, and we have entered the implementation phase of enterprise blockchain adoption.

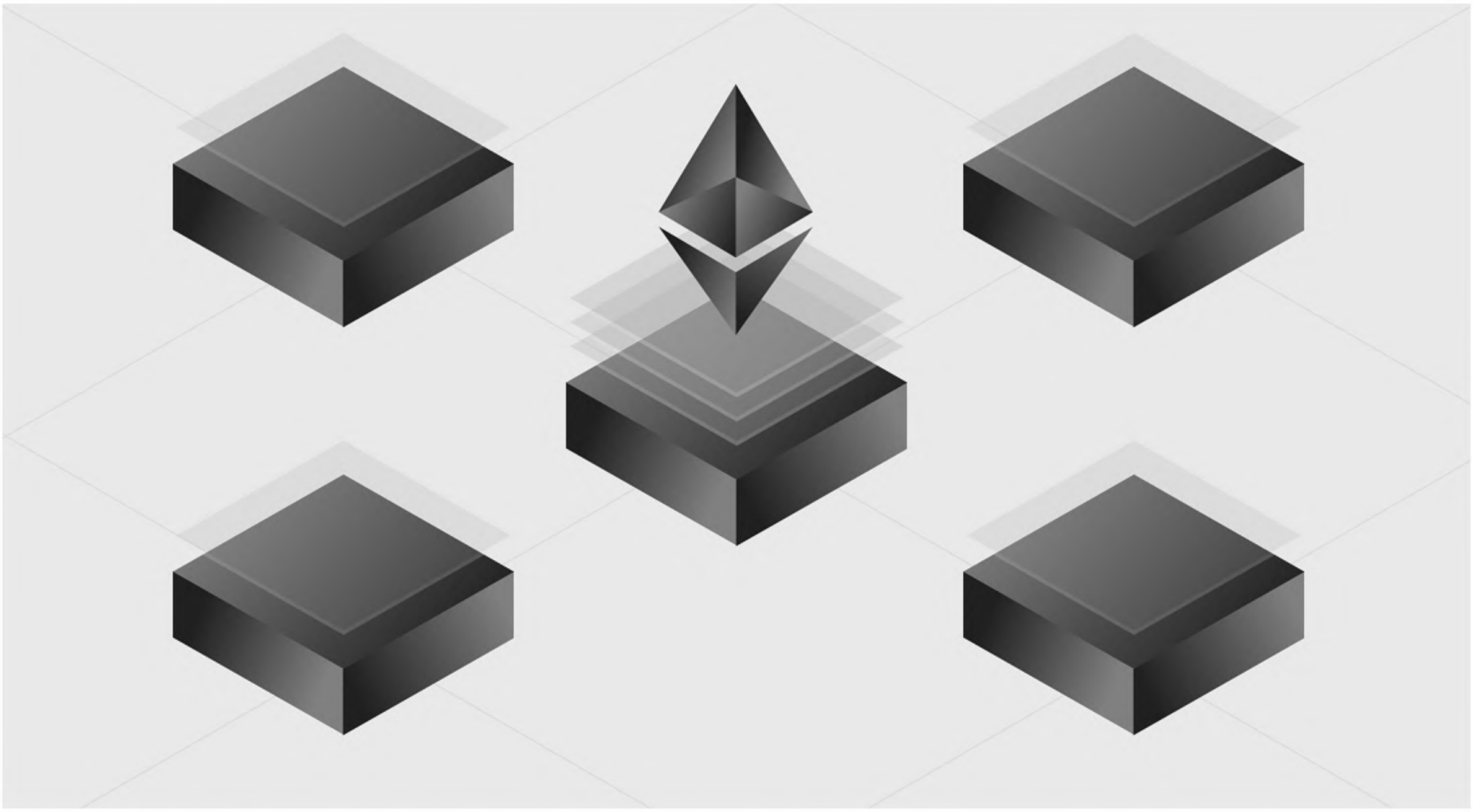
Regulation is also catching up, which reduces uncertainty. Europe's MiCA (Markets in Crypto-Assets) framework is live. Singapore and Hong Kong are approving real tokenized financial products. In the United States, the GENIUS Act (which provides a regulatory framework for stablecoins) passed, and the CLARITY Act (which provides regulatory clarity for numerous facets of the crypto industry) is advancing, removing significant regulatory ambiguity. Even central banks are piloting digital currencies on Ethereum testnets, pulling governments themselves into the ecosystem.

At the same time, there's a generational handoff underway. A new class of executives and investors view blockchain not as a speculative toy but as core market infrastructure. For these leaders, the debate isn't whether to use blockchain, but how best to implement it. Those who move early will gain a compounding advantage. Standards for tokenized securities, onchain identity, and cross-chain interoperability are being defined now. Institutions that take action today will shape these standards and capture the new markets that form around them. Those who wait risk being left to adapt to rules they didn't write. Industry leaders like Apollo, Franklin Templeton, BlackRock, J. P. Morgan, and Société Générale are already in production with blockchain-based solutions, while most others remain stuck in pilot projects.

Ethereum is transforming financial infrastructure. But it's not just about using Ethereum's base layer. Layer 2 infrastructure is the toolkit that makes this transformation practical: the environment where scalability, privacy, and customization turn pilot projects into production systems. The time to understand and embrace Ethereum L2s is now.

What are Layer 2s?

Ethereum is a global settlement and execution layer—a neutral, secure piece of public digital infrastructure where applications run and their activity is recorded and finalized. Think of it as a digital city: it supplies the roads, utilities, and building codes (the shared computing, data, and rules) so anyone can open and operate businesses or services side by side, from decentralized finance to stablecoins and tokenized real-world assets, all inheriting a unified base of trust and interoperability. From the beginning, Ethereum's architecture was designed to be extensible. This was not just for technical flexibility, but also for practical business reasons: it was understood that a single chain could not optimally handle every use case at scale.



Layer 2 (L2) networks build on that idea. They take Ethereum's core strengths—security, neutrality, and a massive developer ecosystem—and expand what can be built on top of it. L2s allow enterprises to design blockchain environments tailored to their own requirements for privacy, compliance, performance, or cost, without needing to create an entirely new blockchain from scratch. Rather than replacing Ethereum, L2s work alongside it. Transactions are processed off the main chain (on an L2 network, which can be public or permissioned), then bundled together and periodically settled on Ethereum. In this way, Ethereum remains the anchor of trust and security (all the batched results are ultimately verified on the mainnet), while L2s provide the scalability and adaptability for day-to-day operations.

Over the last several years, more than a hundred teams have experimented with building their own L2 networks, customizing the architecture to their needs. Some have introduced custom fee tokens or different execution environments; others have added compliance features or alternative consensus mechanisms. Crucially, these projects could focus on their specific market fit because they could rely on Ethereum to provide the base security and stability. The result is a rich L2 landscape that inherits Ethereum's robustness but offers myriad options for optimization.

The Layer 2 architecture offers significant advantages for enterprises and institutions. L2s enable high-volume transactions (suitable for use cases like payments, gaming, or high-frequency trading) at a fraction of mainnet costs. They facilitate systems with tailored access control, privacy settings, and compliance features. And because L2s still ultimately record data or proofs on Ethereum, they maintain an anchor to a public, immutable ledger, giving assurance that the records are tamper-proof. In short, L2s provide a way to scale and customize blockchain solutions while leaning on Ethereum for what it does best: secure, neutral settlement.

Layer 2s vs. Sidechains and Alternative L1s

Before moving further, it's important to distinguish Ethereum's Layer 2 networks from sidechains and alternative Layer 1 (alt-L1) blockchains. While L2s are tightly coupled to Ethereum and derive their security from it, sidechains and alt-L1s are entirely separate blockchains. First, a couple of definitions: a sidechain is a blockchain that runs in parallel to a main chain (like Bitcoin or Ethereum), but is connected by a two-way bridge and is often designed as a scaling solution for the main chain. An alt-L1 is a completely independent, standalone blockchain network that handles its own security, consensus mechanism, and transaction validation from the ground up and is often viewed as more of a market competitor.

A sidechain or alt-L1 may be compatible with Ethereum's technology (for example, using the same programming engine, the EVM), but it does not inherit Ethereum's security guarantees. This means that assets or transactions on a sidechain rely on that sidechain's own security and validators (which are often significantly less decentralized or less secure). In a worst case scenario, a sidechain could even be controlled by a single operator, making it vulnerable to censorship or fraud. In essence, using a sidechain introduces additional trust assumptions: you must trust the sidechain's validators or operators, since Ethereum's security will not protect those assets.

Layer 2 networks, by contrast, are not standalone blockchains, but rather extensions of Ethereum. They integrate seamlessly with Ethereum's security and infrastructure. If a malicious transaction or network malfunction occurs on an L2, the Ethereum mainnet acts as a neutral, independent referee. It can reject any invalid state updates that an L2 tries to finalize. Furthermore, an L2 can be designed so that users always retain the ability to withdraw their funds back to the Ethereum mainnet, even if the L2 operator fails or becomes uncooperative. This built-in escape hatch ensures that no counterparty (even an L2 operator or consortium) can unilaterally restrict access to assets. For institutional participants like banks, this assurance is critical: they get the flexibility of a custom network without the risk of being "stuck" in a proprietary system.

In summary, sidechains/alt-L1s may offer some scalability or custom features, but they sacrifice the trusted security of Ethereum. Layer 2s preserve that trust by design. Ethereum and its L2s work in tandem: Ethereum provides the foundation of trust and finality, while L2s provide speed and customization. This relationship is fundamental to why L2s are viewed as the strategic path for scaling Ethereum for widespread use.

Types of Layer 2 Solutions

There are multiple kinds of L2 implementations, each with different approaches to validating transactions and ensuring security. The most common L2s today are known as rollups, of which there are two main types:

Optimistic Rollups

These assume transactions are valid by default (optimistically) and post periodic state commitments to Ethereum (a cryptographic summary of the L2 state, including all account balances and contract states). The rollup's transactions are considered final unless fraud is detected. If an invalid transaction slips through, there is a window of time during which participants can challenge it by submitting a fraud proof. In case of a valid challenge, Ethereum will reject the fraudulent state. All data needed to reconstruct the L2's state is usually posted on Ethereum, ensuring anyone can verify the rollup's activity independently. Optimistic rollups inherit Ethereum's security in that Ethereum can revert any fraud that is proven within the challenge window. The trust assumption is minimal: one must trust that at least one honest party will challenge any invalid transactions (and the mechanism is set up to incentivize this).

Zero-Knowledge Rollups (ZK rollups)

These use advanced cryptography to prove the correctness of batched transactions. Instead of relying on challengers, a ZK rollup produces a validity proof (using zero-knowledge proof techniques) that mathematically guarantees all transactions in the batch are valid and follow the rules. This proof is submitted to Ethereum, and Ethereum's smart contracts verify it before accepting the new state. Like optimistic rollups, ZK rollups also post the transaction data (or enough data to reconstruct state) on Ethereum for transparency. The security guarantees are also very high: if the proof verifies, the state is valid by definition, and Ethereum enforces it. Trust assumptions are minimal: operators are essentially relying on the soundness of the cryptographic proof system (and the proper setup of the zk system). The advantage of ZK rollups is that there's no need for a long challenge period to detect fraud—withdrawals and finality can be achieved much faster because validity is proven upfront.

There are other variants of L2s beyond these rollups, each making different trade-offs between scalability, security, and trust assumptions. For example:

Validiums

Similar to ZK rollups in that they use zero-knowledge proofs for validity, but they do not post all transaction data on Ethereum. Instead, data is kept with an external data provider (off-chain). Ethereum still gets a validity proof to ensure transactions are correct, but because the data isn't on Ethereum, users must trust that the external data availability provider will supply the data if needed. This results in a moderate security guarantee: the transaction computations are correct (thanks to ZK proofs enforced by Ethereum), but if the data provider disappears or withholds data, it could halt the ability to fully verify or withdraw. Thus, additional trust is placed in the data provider's integrity.

"Optimiums"

(a less common term, essentially optimistic chains with external data). These are analogous to Validiums but in the optimistic realm—they rely on fraud proofs for correctness but do not store all data on Ethereum. Instead, like Validiums, they depend on an external data availability source. The security is similarly moderate: as long as the external data source is honest and available, fraud proofs can be issued to correct any bad transactions. But if the data source fails, users might be unable to prove fraud or retrieve their funds, so there's a higher trust assumption on that provider.

In all cases, the key differences among L2 types often come down to how data is made available and how state is validated. Rollups (both optimistic and ZK) are currently the gold standard because they keep Ethereum in the loop for both data and validation, minimizing new trust assumptions. Other constructions can offer performance or cost benefits but introduce additional trust in off-chain components. The Ethereum community tracks these nuances closely—resources like L2BEAT (a Ethereum Layer 2 focused analytics site) provide comprehensive breakdowns of the different L2 designs and the risks associated with each.

Data Availability

Data availability is a foundational aspect of any Layer 2. The term refers to whether transaction data can be reliably accessed and reconstructed by participants, even if an L2 operator goes offline or acts maliciously. In simpler terms: if something goes wrong on the L2, is all the information needed to verify transactions and recover assets still obtainable from the public record?

Different L2 designs handle data availability differently, and this choice has huge implications for security and trust:

For rollups (both optimistic and ZK rollups), data availability is achieved onchain. Every batch of transactions posted to Ethereum includes either the raw transaction data or a compressed form of it. Because Ethereum stores this data, anyone can later use it to reconstruct the L2's state from scratch if necessary. This provides maximum transparency and security—even if the L2 operator disappears, the state can be recovered and verified from Ethereum's records alone.

For solutions like Validiums or other external-data L2s, the transaction data is kept on an external data availability (DA) provider (which could be a set of nodes, a specialized network, or even a permissioned committee). In these cases, Ethereum might store a hash or proof of the state, but the full transaction details live elsewhere. The validity proofs (in ZK systems) or fraud proofs (in optimistic systems) can still be posted to Ethereum to confirm correctness of state transitions. However, if the external DA provider fails or refuses to cooperate, new users cannot reconstruct the full state or verify all transactions independently. This creates an extra trust assumption: you must trust the external provider to always supply the data when needed.

Data availability is critical because it underpins the ability to audit and trust an L2. High data availability (as in onchain data) means anyone can audit the L2's history, transactions can be verified without asking permission from any party, and users have an assurance they can exit to L1 Ethereum if needed (since the data to prove their state on L1 is available). Lower data availability (off-chain data) can improve efficiency and throughput, but relies on the honest behavior of whoever holds the data.

In general, enterprises should carefully review an L2's data availability setup, because it affects security, regulatory compliance, and auditability. A system with poor data availability may not meet strict requirements for independent audits and data retention policies that many institutions have.

In general, data availability plays a big role in an L2's security guarantees, and its setup should be carefully reviewed, particularly as high data availability also relates to enabling automated audits and meeting compliance regulations, which are highly relevant for institutional applications.

To summarize the differences among L2 approaches, below is a quick overview of the main categories and their properties:

Category	Data Availability (DA)	State Validation	Security Guarantee	Trust Assumptions
Optimistic Rollups	Onchain (Ethereum)	Fraud Proofs	**High** (Ethereum can revert fraud)	**Minimal** (relies on the possibility to make a state challenge)
ZK Rollups	Onchain (Ethereum)	Zero-Knowledge Proofs	**High** (ZK + L1 enforcement)	**Minimal** (relies on the correctness of ZK proofs)
Validiums	External	Zero-Knowledge Proofs	**Moderate** (correctness on Ethereum, but data availability external)	**High** (DA provider integrity)
Optimiums	External	Fraud Proofs	**Moderate** (depends on DA provider, not L1)	**High** (DA provider integrity)

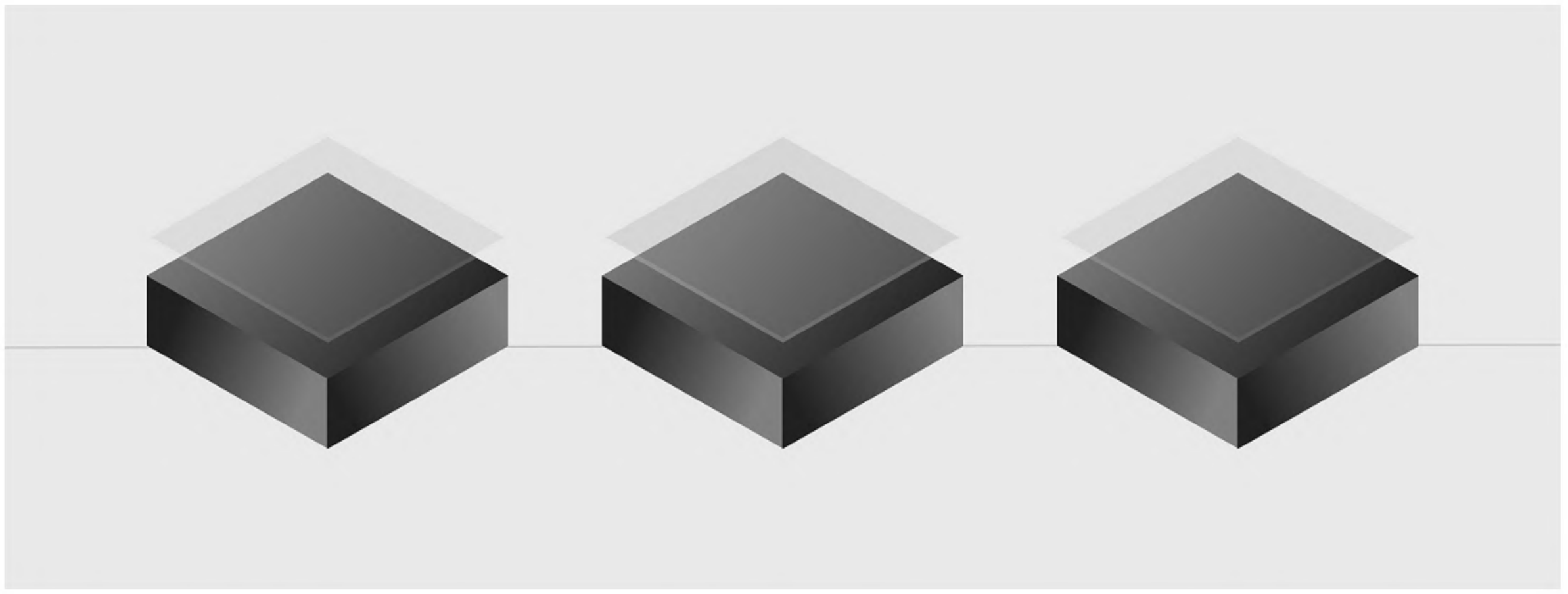
The takeaway is that rollups (optimistic or ZK) provide the strongest guarantees by anchoring both data and verification on Ethereum. Other L2 constructions can be useful for certain applications but involve trade-offs that should be understood. Many institutions may gravitate towards rollup-based solutions to minimize new risks, especially for high-value or highly regulated use cases.

How Ethereum Layer 2s Address Institutional Needs

From an enterprise perspective, adopting any technology means evaluating how it meets core requirements: ownership and control, customizability, privacy, speed, compliance, reliability, and cost-effectiveness, to name a few. Ethereum's base layer provides an excellent foundation, and L2s extend it with the flexibility required for production-grade use in financial markets. Below, we examine several key areas through an institutional lens and how Ethereum L2 solutions address them.

Ownership and Control

Institutions looking into blockchains often ask: should we use a shared public network, or run our own infrastructure? With Ethereum L2s, they don't have to choose between one or the other. Building or owning their own L2 network gives institutions a level of control and customization that isn't possible on a one-size-fits-all public blockchain alone, while still benefiting from Ethereum's public settlement layer.



By operating their own L2, a bank, exchange, or asset manager can dictate the network's parameters: for example, how transactions are sequenced, how and where data is stored, who can access the network, and how compliance rules are enforced. They can integrate their L2 with internal governance processes, ensuring that changes to the system follow the organization's risk management and change-control policies. All of this is done while anchoring security and final settlement to Ethereum—meaning they don't sacrifice the trust and connectivity that comes from being on the global Ethereum platform.

Owning an L2 unlocks several advantages:

Regulatory alignment

Infrastructure can be tailored to meet regulatory requirements in specific jurisdictions (e.g., certain data may be kept private or stored in-region, certain participants can be whitelisted or excluded, etc.).

Privacy and confidentiality

Sensitive business data or client information can be shielded from the public, only revealed on a need-to-know basis (we discuss more under *Privacy* below).

Guaranteed service levels

By controlling the sequencer (the node or set of nodes that order transactions on the L2), an institution can ensure high availability and performance, similar to how they manage other mission-critical systems. They can also commit to service-level agreements for their clients using the platform.

New revenue streams

Running an L2 means the institution isn't just a user of someone else's network—it becomes the network operator. This opens up potential revenues from transaction fees (sequencer fees), priority services, or specialized functionality offered to partners and clients.

Customization of execution environment

Institutions can experiment with custom features (like specialized smart contract functions, unique fee structures, or integration with existing systems) without needing permission from a larger public network. They have a sandbox to innovate, with Ethereum's base layer ensuring the outcomes remain interoperable with the broader ecosystem.

Importantly, owning an L2 does not mean isolation from the rest of the market. These networks can interoperate with Ethereum and other L2s, preserving access to global liquidity and the broader DeFi ecosystem. An institution's L2 can be permissioned and controlled for internal use, yet still connect via bridges to the public Ethereum network when needed (under the institution's terms). In effect, Ethereum L2s let institutions operate with the confidence, predictability, and control of traditional systems, while still enjoying the connectivity and innovation of the open blockchain network.

Privacy and Confidentiality

Financial institutions cannot operate in an environment where every trade or client balance is exposed to the entire world. Privacy and confidentiality are paramount for things like trading strategies, customer identities, and business-sensitive data. Ethereum L2 solutions recognize this need: they allow for private transactions or networks while still benefiting from Ethereum's public security umbrella.

On L2s, various techniques can be employed to keep data confidential:

Some institutional L2s are permissioned, meaning only approved participants can access them, and transactions are not visible to outsiders. This is akin to a private consortium blockchain, but again with the advantage that final settlement can still occur on Ethereum (providing an immutable audit trail when needed).

Even on public L2s, selective disclosure is possible. A transaction's details can be hidden, yet certain parties (like regulators or auditors) can be given viewing privileges or proofs that the hidden transaction met required conditions.

One groundbreaking technology enabling onchain privacy is zero-knowledge proofs (ZK proofs). Zero-knowledge proofs allow one party to prove to another that a statement is true, without revealing why it's true or any of the underlying data. In practice, this means you could confirm that a transaction or a user meets certain criteria (for example, passes all KYC/AML checks or stays within trading limits) without exposing the actual details (like the user's identity or the amounts).

Using Zero-Knowledge Proofs for Privacy: Projects like EY's Nightfall, ZKsync's Prividiums and Scroll's experimental Cloak illustrate how ZK proofs can facilitate private transactions on Ethereum and L2s. For example, an institution could utilize ZK technology to ensure a bond trade between two parties is compliant with regulations (KYC, AML, sanctions screening, etc.) and within allowed limits, without publicly revealing the identities of the parties or the trade details. The blockchain (and regulators with the right keys) gets a cryptographic confirmation that "all rules were followed in this transaction," and nothing more. Clients maintain confidentiality, competitors can't see sensitive positions, and yet regulators are satisfied because they can be given the tools to verify compliance when needed. This capability means blockchains can move away from the misconception that everything must be public—instead, they can offer privacy by design, with the option of transparency for those who require it (regulators, auditors) via controlled disclosure or viewing keys.

In summary, L2 solutions enable a spectrum of privacy options. Institutions can operate in a mode where, to the outside world, little or no sensitive data is visible onchain, but the necessary parties can still get evidence of compliance and the system still benefits from Ethereum's security. This balances the openness of blockchain with the confidentiality demands of finance.

Data Availability, Storage, and Auditability

Enterprises operate under strict requirements for record-keeping, data retention, and auditability. Regulators demand that transaction records be preserved for years and that firms can produce an auditable trail of activity. Ethereum's design (especially with L2s) provides new ways to meet these needs with greater assurance and less manual effort.

Data Availability for Compliance

As discussed earlier, data availability determines whether historical transaction data can be retrieved and verified. Institutions need immutable records for regulators and auditors, but they also need flexibility in how and where data is stored. L2s can be configured for different data availability models. Some publish all transaction data to the Ethereum mainnet (maximizing transparency and permanence), while others use specialized data networks. For instance, an emerging solution is EigenDA—a dedicated data availability layer that can work alongside Ethereum to ensure transaction data is published and retrievable during settlement, without cluttering the L1 with bulk data. These data layers are not meant for indefinite storage of every byte of data, but they guarantee that if someone needs to verify a transaction or rebuild state (e.g. during a compliance check), the necessary data will be there or can be proven. This drastically reduces the need for manual reconciliation because the source of truth is always available onchain or on a complementary, always-online system.

Data Storage

While data availability mechanisms ensure that transaction data is accessible at time of settlement, data storage is about preserving and archiving records long-term. Blockchains themselves (even Ethereum and its L2s) are not optimized for large-scale data storage of detailed transaction records over decades. However, institutions can combine blockchains with off-chain storage to achieve the best of both. For example, an organization might maintain its own internal data warehouse or archive that captures every transaction detail from its L2 in real-time. Additionally, decentralized storage networks like Filecoin or Arweave can be leveraged via smart contracts to store encrypted transaction logs or documents in a tamper-proof, decentralized manner. These solutions provide programmatically verifiable records (thanks to cryptographic hashes and proofs) without relying on a single centralized database or creating a single point of failure. Years after a transaction, an institution could retrieve the record from decentralized storage and verify its integrity against the blockchain's hash of that data.

Auditing and Reporting

By combining the above—onchain data availability and robust storage—L2-based systems make auditing far more powerful and efficient. In traditional finance, auditing involves sampling records, trusting internal databases, and extensive reconciliation between parties. With Ethereum and L2s, every transaction is anchored to an immutable ledger, and cryptographic proofs can verify the completeness and authenticity of records. Regulators or auditors could be given a cryptographic proof or a viewing portal that shows that every transaction in a given period met certain criteria, with significantly less room for human error or manipulation. Instead of relying on after-the-fact reconciliation and paper trails, audits can be done by verifying mathematical proofs and hashes.

For institutions, this means reporting can shift from a slow, manual process to a nearly real-time, automated one. Compliance teams can get continuous assurance from the system itself. Regulators, in turn, gain a stronger framework: rather than trusting an institution's internally prepared reports, they can independently verify activity at the protocol level. The net result is an infrastructure where auditability is built-in, not bolted on. This lowers operational risk, reduces compliance costs, and increases trust between institutions and regulators.

Cost Reduction and New Revenue Opportunities

At the end of the day, financial institutions care about economics. Blockchain technology must prove that it can either save money or generate new revenue (ideally both). Ethereum L2s deliver on the cost side by making transactions dramatically cheaper, and they also open the door for new revenue streams through ownership of infrastructure.

Lower Transaction Costs

Public blockchains like Ethereum mainnet historically had high fees during peak usage, which is impractical for many enterprise uses. L2s solve this by batching thousands of transactions and settling them as a single transaction on Ethereum. The overhead cost of using Ethereum is then split across many transactions. In practical terms, what might cost a few dollars to do on Ethereum might cost only a few cents (or less) on an L2, depending on volume. This is a game-changer for high-volume use cases like payments, trading, or consumer applications—suddenly blockchains become cost-competitive with, or even cheaper than, legacy systems. For an industry that spends billions annually on payment processing, clearing, and settlement, these savings are significant and directly improve the bottom line.

Turning Costs into Profit Centers

Cost reduction is only half the story. By running their own L2 networks, institutions can transform their back offices from a cost center into revenue-generating infrastructure. Consider a bank that normally just pays fees to use someone else's network: if instead it operates the network (the L2), it can earn the fees. The bank could charge transaction fees or offer tiered service levels (e.g., guaranteed low latency for certain customers, or integration services) on its L2. It could also design the fee model, perhaps charging in its native fiat or a stablecoin and managing how those fees are allocated or burned. The L2 sequencer role could be analogous to an exchange being the market operator: it's an opportunity to capture value from the activity happening on the platform.

In summary, Ethereum L2s can reduce costs per transaction by orders of magnitude and at the same time enable forward-looking institutions to participate in the economics of the network itself. This can increase profit margins on existing services and create entirely new business models around blockchain infrastructure.

Customizability with Composability

In technology, there is often a trade-off between building a bespoke system that perfectly fits your needs (but is siloed) and using a common system that connects you with everyone else (but may not fit your needs exactly). Ethereum L2s offer a rare combination of customizability and composability, allowing institutions to tailor their environment as they wish, while still being able to interact with the wider financial ecosystem.

Customizability : Every institution has slightly different requirements. A global bank issuing tokenized bonds might need fine-grained permissions and compliance checks on who can hold those bonds. A supply chain platform might need privacy for commercial transactions and the ability to handle occasional off-hours bursts of activity. A corporate treasury might want an internal stablecoin network with specific controls on minting and redemption. L2s let each institution or consortium create an execution environment optimized for these needs. They can implement permissioned bridges so only whitelisted assets or users can enter, they can enforce custom rules at the smart contract level (for example, preventing certain asset transfers unless both parties are KYC-verified) and they can optimize performance parameters (block times, transaction formats, etc.) for their use case.

Composability (Interoperability): Despite this customization, L2s remain composable with the broader Ethereum ecosystem. Composability means that applications and assets on the blockchain can seamlessly interact with each other like Lego pieces. By anchoring to Ethereum, an institution's L2 can tap into Ethereum's global liquidity and network of services whenever needed. For instance, a tokenized security issued on a private L2 can still be bridged to Ethereum mainnet or another L2 to be traded or used as collateral in DeFi (subject to whatever constraints the issuer wants to impose). If a company builds a supply chain financing app on an L2, it can still use Ethereum's stablecoins for settlement and maybe even connect to insurance protocols or identity solutions on Ethereum.

This combination is powerful: institutions no longer have to choose between a closed system and an open network. They can have a closed, controlled environment for day-to-day operations and sensitive data, but with doors that open to the wider market when they want to interact or exchange value. For example:

In capital markets, a bond might be issued and traded within a private rollup accessible only to regulated broker-dealers. However, when needed, that bond's tokens could be moved onto a public L2 or mainnet to be used in broader financial transactions or to allow a different set of investors to participate, all under the issuer's control.

In supply chain finance, transactions between manufacturers, suppliers, and financiers can happen on a private L2 to protect trade secrets. Yet, the final settlement of payments can occur via a public stablecoin on Ethereum, and the participants can still use public identity attestations or insurance services from Ethereum's ecosystem.

For payment networks, a corporation might run its own L2 for internal transfers and employee payroll using a corporate stablecoin. This L2 could enforce privacy and limit access, but the stablecoin itself could be made interoperable so that, if needed, employees or subsidiaries can transfer value out to the wider Ethereum network (for instance, to pay a vendor externally), all while respecting compliance.

L2s let institutions have their cake and eat it too. They can design a blockchain-based system that fits their requirements exactly (something not possible if you only use the shared Ethereum mainnet), while keeping one foot in the larger, open Ethereum world, ensuring they are not building siloed infrastructure. This balance—tailoring an environment to specific needs while preserving the ability to compose and integrate with everything else—is what turns Ethereum from just a public blockchain into a truly flexible foundation that institutions can shape to fit their own markets.

Compliance and Regulatory Alignment

Compliance is the gate that institutional adoption must pass through. No bank or enterprise can embrace a new infrastructure if it cannot meet regulatory requirements and internal risk controls. The good news is that Ethereum and its L2s are increasingly aligning with these needs through both technology and legal clarity.

On the technology side, onchain identity and compliance tools have matured significantly. It's now possible to enforce compliance before transactions occur, rather than just reporting on them after the fact. For example, identity frameworks can attach attributes or credentials to blockchain addresses (wallets). A wallet can carry a proof that "Owner has passed KYC and is a US accredited investor," without revealing the owner's actual identity onchain. Smart contracts can check these credentials automatically and block non-compliant actions. This means a transfer of a token can be prevented from executing if, say, the receiving wallet isn't approved for that type of asset or if doing so would break a sanctions rule. Instead of relying on off-chain processes and hoping users follow the rules, the rules are baked into the asset's logic.

Onchain Compliance Tools

Instead of running KYC or AML checks after a transaction has been executed, onchain identity frameworks now make it possible to enforce rules before assets move. Wallets can carry verified credentials or attestations that confirm an entity has passed necessary checks, without exposing personal data to every participant in the network. Smart contracts can be programmed to block non-compliant activity automatically, reducing both regulatory risk and operational overhead. For institutions, this represents a shift from monitoring to proactive enforcement. Compliance isn't an afterthought anymore, it is built into the applications themselves.

Legal Frameworks

Technical tooling is advancing at the same time as the legal environment is solidifying. Europe's MiCA framework now provides a comprehensive regulatory structure for digital assets, giving institutions a clear path to launch compliant tokenized products. In the United States, the GENIUS Act has established a path for fully reserved, dollar-pegged stablecoins, and the CLARITY Act is set to provide even broader certainty for digital asset operations. In Asia, regulators in Singapore and Hong Kong are actively approving pilots under sandbox regimes. Blockchain has moved from a gray zone to an environment of actionable regulatory clarity. Ethereum is the chain where compliant solutions are already being tested and deployed at scale, making it the natural foundation for institutions looking to move first.

In summary, compliance is no longer a blocker to Ethereum adoption at scale; it's becoming an enabler. The combination of onchain compliance technology and clear regulations means institutions can meet their legal obligations on Ethereum L2s often more effectively than in traditional systems (since blockchains can provide better transparency and audit trails). We are moving from an environment of uncertainty to one of actionable clarity, where a bank can say: "Yes, we can issue this asset or run this process on Ethereum within the rules."

Case Studies and Early Models

These trends aren't just theoretical—some of the world's leading institutions are already leveraging Ethereum and L2s to solve real problems:

J.P. Morgan

Piloting deposit tokens (tokenized bank deposits) on Base, an Ethereum L2 operated by Coinbase. This trial aims to improve settlement speed and interoperability for the bank's wholesale payments and could lay the groundwork for large-scale institutional payment networks on L2s.

Visa

Experimenting with zero-knowledge proofs to enhance privacy in tokenized asset platforms. Visa has prototyped how an employer could use an L2 to issue tokenized obligations (like salary payments or benefits) and use ZK proofs so that only the necessary parties see transaction details, protecting client privacy.

Société Générale (Forge)

Launched euro- and dollar-backed stablecoins on Ethereum under the MiCA framework. This marked one of the first instances of a major global bank issuing its own regulated digital money on a public blockchain, demonstrating confidence in Ethereum's ability to meet compliance and security standards.

These examples show that enterprises can leverage Ethereum and its L2s today to address pressing needs like settlement efficiency, privacy, and new digital product offerings. They are leading the pack, but many others are poised to follow as pilot programs mature into production systems.

The Established Operating Model

Having understood the why and what of Ethereum L2s, the next considerations are how to implement these solutions in practice. This section outlines a high-level operating model for using Ethereum with L2s, and provides guidance on selecting the right L2 environment and managing deployment and operations. In essence, it's about translating the promise of Ethereum L2s into a concrete strategy and action plan for an institution.

Selecting Your Infrastructure

Layer 2 Environments and Applications

The term "Layer 2" encompasses a variety of networks and configurations. Choosing the right one is a strategic decision that depends on an institution's goals and constraints. Broadly, an organization will consider whether to use an existing public L2 or to set up a private/permissioned L2, and whether to opt for an optimistic or ZK-based solution.

Public vs. Private L2s

Public L2s (examples include Optimism, Arbitrum, Linea, among others) are open networks built on Ethereum that anyone can use. They deliver broad market reach and immediate access to liquidity. By using a well-known public L2, an institution can tap into an existing user base, standardized tooling, and established DeFi protocols on that L2. Transaction costs on public L2s are typically very competitive due to scale and the fact that multiple user bases share the network. Another advantage is that many public L2s have identifiable operators or foundations, which means an enterprise can engage with them for support, service-level agreements, or to discuss feature roadmaps. Use cases: Public L2s are often well-suited for applications like retail payments, consumer-facing applications (where you want to be where users already are), or any scenario where open liquidity and high throughput are priorities (e.g., a high-frequency trading platform connecting to many counterparties).

Private or Permissioned L2s are bespoke networks where access is restricted to certain participants (or fully controlled by one entity). These are essentially custom rollups or L2 chains that an institution runs for itself or a consortium. They address needs around confidentiality, governance control, and regulatory compliance that a public network might not meet. On a private L2, the institution can enforce that only whitelisted addresses participate, implement granular access controls, hide transaction details from anyone not authorized, and integrate specific regulatory reporting features (like automatic reporting of certain transactions to a regulator off-chain). Settlement integrity still remains anchored to Ethereum (for security and future interoperability), but everything else can be tuned. Use cases: Private L2s shine in scenarios like private markets (e.g., a private exchange for unlisted securities among invited brokers), institutional trading workflows (where trades are confidential but need eventual public settlement), or internal bank operations (like inter-company transfers, syndicate loan management, etc., where privacy and control are paramount).

Optimistic vs. ZK Rollup Architectures

Optimistic Rollups prioritize simplicity and compatibility. They use the fraud-proof model, which is generally easier to implement and maintain in the short term. Most EVM-compatible optimistic rollups can leverage existing Ethereum developer tooling with minimal changes (smart contracts often deploy as-is). The trade-off is the challenge period for exits: typically, users withdrawing funds from an optimistic rollup back to Ethereum must wait (often around 7 days) to allow time for any fraud challenges. If your use case can tolerate that (for example, if immediate withdrawal isn't critical or there are liquidity providers to bridge faster), optimistic rollups are a solid choice.

ZK Rollups offer quicker finality on withdrawals (as soon as the proof is accepted, which could be minutes), because they don't rely on game-theoretic challenges—they rely on math proofs. They also potentially offer higher throughput in the long run and can enable some privacy features. However, ZK rollups involve more complex technology (developing the circuits and proofs) and sometimes higher computational overhead (generating proofs is heavy, though improving). Compatibility with existing Ethereum code is improving (projects like ZKsync aim for general EVM compatibility), but may not be 100% for all edge cases yet. If an institution values fast finality and is okay with a newer technology, ZK rollups are an attractive option.

In practice, the choice often boils down to settlement speed requirements and technology maturity. If you need the absolute fastest finality and are dealing with high volumes (and you have the expertise to manage a ZK system), a ZK rollup might be preferred. If you want something battle-tested with broad compatibility today, optimistic may be the way to go. It's worth noting that the gap is closing as ZK tech matures, and some organizations are betting on ZK as the future for all L2s.

Infrastructure Selection Framework - Key Evaluation Criteria

When evaluating specific L2 options (whether joining a public L2 or launching your own), institutions typically consider several key dimensions:

Market positioning

Does the L2 align with the markets and liquidity pools you need? For a trading application, being on an L2 that already hosts major exchanges or market makers could be beneficial. For a consumer app, an L2 with a large user base (wallets, NFTs, etc.) might make adoption easier.

Economic model

Evaluate the fee structure and throughput. Are there any token incentives or costs (some L2s might have their own token for fees or security)? Does the L2 throughput (transactions per second capacity) meet your requirements during peak times? This analysis ensures that the solution is financially viable at scale.

Compliance architecture

Does the L2 support the compliance features you require? For example, can it integrate with identity/KYC systems? Does it support permissioned access or whitelisting of addresses if needed? If your data needs to stay in certain geographic regions (data residency rules), can the L2 accommodate that (perhaps via regional sequencers or specific data centers)? Essentially, you verify that using the L2 won't break any regulatory obligations and ideally that it makes compliance easier.

Operational Accountability

For any external L2 provider, consider the operational support and guarantees. Is there an identifiable operator or organization behind the L2 who can provide uptime commitments, support, and perhaps custom SLAs? If an institution is going to rely on an L2 for mission-critical operations, they may prefer networks where there's a professional team that can be engaged, as opposed to an experimental network run by volunteers. Ideally, there should be a known party responsible for updates, responding to incidents, etc., in a transparent way.

Integration Readiness

Check the available tooling and integration points. Does the L2 work with the wallet infrastructure you expect to use (e.g., does it support popular hardware wallets or custodial systems out of the box)? Are there APIs or SDKs to connect your existing systems? If you need fiat on/off ramps, are there providers integrated on that L2? How easy is it to integrate your compliance monitoring or reporting tools? High integration readiness means shorter deployment time and fewer surprises.

Strategic Flexibility

Consider the long-term strategy. If you start on one L2, how easy is it to migrate to another or to adjust if conditions change? Ideally, using Ethereum L2s keeps you flexible; if the L2 you choose becomes too expensive or less optimal, you could move assets to a different L2 or to mainnet since everything is ultimately compatible via Ethereum. Ensure that whatever choice you make preserves the ability to pivot without stranding assets or users. Using standard token standards and bridges (or being able to deploy your own bridge) can be part of this consideration.

One additional criterion might be security track record: examine whether the L2 has undergone audits, what its bug bounty program looks like, and how it has handled any past incidents. Enterprises will favor solutions that have demonstrated robustness.

After weighing these factors, an institution may decide to join an existing public L2, collaborate on a consortium L2, or build its own dedicated L2. All are viable paths—the decision depends on where the institution finds the best mix of control, cost, and connectivity.

When Ethereum Mainnet Provides Optimal Value

It's worth noting that in some scenarios, an institution might opt to conduct activities on Ethereum mainnet itself rather than an L2. Ethereum L1 offers maximum security and the broadest reach, which is ideal for certain functions:

Canonical asset registries

The definitive record of asset ownership, identity registries, or governance records are often best kept on mainnet to ensure universal acceptance and permanence. For example, one might record the master record of a bond issuance on mainnet, even if trading happens on L2.

Regulatory and audit anchors

Any public disclosures, reference data, or audit evidence that needs to be openly verifiable by third parties (and expected to remain accessible for decades) could be put on mainnet. This could include hash fingerprints of reports, or certain compliance transactions that regulators want on a public ledger.

High-value settlement

Very large transactions, or those involving critical collateral or escrow, might be settled on L1 for the highest security assurance. If you're moving $500 million in a single transaction between institutions, doing it on Ethereum L1 might be acceptable given the fees are negligible relative to value, and you get the strongest finality.

DeFi liquidity and discovery

If you need to interact with the full spectrum of decentralized finance or find a counterparty in an open market, mainnet is where the largest pool of liquidity and participants resides. Some institutions may do an L2 strategy but still occasionally tap mainnet DeFi for specific needs (like sourcing liquidity in a crisis or interacting with a protocol that only exists on mainnet).

Cross-ecosystem bridges

If you are building infrastructure that connects multiple blockchains or L2s (a hub), doing so on Ethereum L1 can be beneficial for neutrality and trust. Many cross-chain bridge projects anchor themselves on Ethereum for this reason.

In summary, Ethereum mainnet remains the ultimate trust layer and should be used when its unparalleled security and decentralization are needed. L2s then handle everything that can be optimized. Most institutional strategies will involve a blend of both: use mainnet where it adds value, and L2 wherever possible to gain efficiency.

Deployment and Operations

Implementing an Ethereum L2 solution is not just about technology choices; it also involves thoughtful planning around deployment, integration, and ongoing operations. Here are some best practices and considerations for a smooth rollout:

Asset Management and Distribution

When issuing or handling digital assets, a recommended approach is to use Ethereum mainnet as the source of truth and then extend those assets to L2 environments as needed. For example, if a bank tokenizes an asset, the authoritative record (token contract) could live on Ethereum mainnet. Then, using standardized Layer 2 bridges, the asset can be "bridged" or transferred onto an L2 for faster trading or use. By doing this, the institution preserves market credibility and unified liquidity—there's only one version of the asset, anchored on Ethereum, rather than multiple siloed versions on different networks.

Avoid creating separate, unlinked tokens on each new platform (which would fragment liquidity and confuse participants). Instead, bridging ensures that whether the asset is on L1 or L2, it's recognized as the same underlying item. This greatly simplifies reconciliation across environments: an asset moved to an L2 can always be moved back or verified against the Ethereum base record.

Additionally, when operating across multiple environments, it's wise to establish change management protocols. If an upgrade or change is needed (say a smart contract update for the asset or a new bridge contract deployment), it is important to set up a system for providing advance notice and perhaps even a maintenance window to all technical teams and counterparties. This mimics how changes are coordinated in traditional finance and avoids surprises that could disrupt activity.

Compliance Integration

Integrating Ethereum and L2 solutions into existing **compliance and governance frameworks** is crucial. An institution should map out how onchain processes will tie into off-chain oversight:

Identity and access

If necessary, make sure identity verification (KYC/AML) is part of wallet issuance or onboarding for your L2. For instance, you might only give L2 accounts or access tokens to users who have been verified through your usual compliance procedures. Link those identities to onchain credentials so that smart contracts can enforce rules as described earlier.

Transaction monitoring

Use or extend blockchain analytics and monitoring tools to cover your L2. There are vendors and open-source tools that can track addresses, flag suspicious patterns, and produce compliance reports for onchain activity just as banks do for traditional accounts. Integrate these with your compliance team's dashboard.

Audit trails

As mentioned, one benefit of blockchain is built-in audit trails. Make sure your compliance and audit teams are trained to understand how to retrieve and interpret onchain records. Providing them with user-friendly tools or interfaces (maybe something that looks like the reports they're used to, but fed by onchain data) will help bridge the gap between new tech and traditional processes.

Private reporting

If certain transactions must be reported to regulators but cannot be public (for confidentiality), design your L2 in such a way that regulators can be given access to the necessary data. This might mean having a node that regulators operate or receive encrypted logs from, or using viewing keys in a zero-knowledge setup. The idea is to fulfill regulatory reporting requirements without exposing sensitive data to the whole world.

Additionally, transparency features like fee attribution can help in accounting. Platforms can provide a clear breakdown of costs per transaction or user, which helps satisfy internal finance and accounting controls.

Economic Planning

When planning a move to an L2, it's important to build a comprehensive cost model that covers all elements of the new architecture:

L2 transaction fees

Even though L2s are cheaper, they are not free. Estimate the costs for the expected volume of transactions on the L2. Many L2s charge fees in ETH or their own token—consider the need to manage and provision those tokens for your operations.

Ethereum settlement costs

L2s periodically post data or proofs to Ethereum. If you run your own L2, you will be paying the gas costs for those posts. Budget for Ethereum gas fees associated with your L2's checkpoints or state commitments. These costs can vary with Ethereum network conditions, so plan for a range.

Operator or service fees

If you're using a third-party L2 (especially if it's run as a service or has a centralized sequencer run by someone else), there might be fees or revenue sharing for that service. Similarly, if you outsource any part of the infrastructure (like using a data availability committee or a cloud service for running nodes), include those costs.

Hardware and infrastructure

Running an L2 (particularly a private one) might involve running validator/sequencer nodes, monitoring systems, and data storage solutions. Calculate cloud or hardware expenses.

Development and maintenance

Developing smart contracts, auditing them, and maintaining the L2 software (applying upgrades or handling any technical issues) is an ongoing expense. This might be factored into overall IT budgets rather than per-transaction costs, but it's part of the ROI consideration: you might need a certain amount of developers and security analysts on staff or contracted to support a blockchain initiative.

Generally, institutions find that for consistent, high-volume transaction flows, Layer 2 solutions deliver far better unit economics than using Ethereum Layer 1 alone or traditional intermediated processes. But due diligence on costs prevents surprises and helps in setting pricing for services offered on the platform.

Governance and Risk Management

Robust governance frameworks with clear authority structures and approval processes are recommended to manage operational and regulatory risks effectively. Partnerships with L2 operators are structured through well-defined contractual agreements that cover data-handling protocols, conflict resolution mechanisms, and performance guarantees. Comprehensive public risk documentation is developed to transparently address withdrawal procedures, centralization factors, security audits, and support resources. Clear, proactive communication significantly reduces regulatory concerns and builds client confidence in infrastructure implementations.

Overview of Major L2 Ecosystems

Ethereum's Layer 2 landscape has evolved into a diverse ecosystem of networks, broadly categorized into optimistic and zero-knowledge based chains as discussed. Most leading L2 projects are now expanding into "network-of-chains" models, essentially creating multiple interconnected L2s to reduce user friction and liquidity fragmentation. For example, the Optimism team envisions a "Superchain" where many rollups share a common infrastructure, while ZKsync is introducing the concept of "Elastic Chains" to allow others to launch their own chains that still plug into ZKsync's ecosystem. These efforts aim to maintain the benefits of specialization (different chains for different needs) while making them feel like one coherent network from a user perspective.

As of today, the most popular Ethereum L2 networks include optimistic rollups like Base, Optimism and Arbitrum, and ZK rollups like Starknet, ZKsync Era, and Linea. Each of these ecosystems has its own strengths and focus areas. Optimism and Arbitrum, for instance, have seen significant adoption in DeFi and gaming, offering EVM compatibility and lower fees. Starknet, powered by STARK proofs, is pushing the envelope on scalability and has a distinct developer community with its Cairo programming language. ZKsync is known for prioritizing user experience (like instant finality), ease of bridging, and enterprise adoption.

It's worth noting that many L2 projects now support launching custom "AppChains" or L3s on top of their infrastructure—the scaling is recursive. For instance, an enterprise could potentially launch its own dedicated chain using the technology of one of these L2s, effectively becoming an L3 that inherits security from the L2 and ultimately Ethereum. This further expands the options for institutions in how they adopt the tech (in some cases, the choice might be between launching an L3 on an existing L2 network vs. a standalone L2).

The L2BEAT website maintains a comprehensive, neutral overview of the adoption, security model, and activity metrics of these various networks. By consulting L2BEAT, one can get up-to-date information on total value locked in each L2, how decentralized they are, what security audits have been done, and other important considerations. This transparency within the Ethereum community helps institutions make informed decisions about which ecosystem to align with.

In summary, the Ethereum L2 ecosystem is robust and growing. Competition and innovation among L2 projects are driving rapid improvements in performance and user experience. Importantly, all these L2s share the common foundation of Ethereum, which means that regardless of which solutions gain the most traction, any investment an institution makes in Ethereum-based tech is future-proofed by the ability to interoperate. As standards mature (for instance, for how L2s communicate or bridge), we can expect using an L2 to become as seamless as using Ethereum itself, but with far greater scalability.

Conclusion

Ethereum and its Layer 2 networks together offer a transformative opportunity for the financial industry. Institutions no longer have to choose between the global reach and neutrality of public blockchains and the control and privacy of private infrastructure—they can have both.

Crucially, the ecosystem and regulatory environment have matured to the point where moving from pilot projects to full production deployment is not only feasible but prudent. The technology is battle-tested, early adopters have demonstrated real use cases, and regulators are providing the clarity needed to proceed with confidence. Those who act now will be in a position to set industry standards, capture new markets, and define the next generation of financial services. Those who delay may find themselves adapting to frameworks and platforms shaped by others.

Ethereum's Layer 2 ecosystem is more than a scalability solution—it is the foundation for a new financial architecture, one that combines the trust of a neutral public ledger with the flexibility of bespoke networks. The rails for the next generation of financial markets are being built today on Ethereum and its L2s. Institutions that recognize this shift and engage proactively will help drive the upgrade of the global economy onto blockchain-based infrastructure, gaining a competitive advantage that will compound for years to come.

About Authors

Etherealize

Etherealize builds Ethereum-based products and infrastructure for Wall Street, delivering compliant, private, and scalable solutions for trading, tokenization, and settlement. Founded in 2025 by Ethereum ecosystem leaders and Wall Street veterans, Etherealize is on a mission to ensure the global financial system is faster, safer, and built for the 21st century.

Nethermind

Nethermind delivers the blockchain infrastructure that enterprise and financial systems depend on. As core Ethereum contributors and builders behind the Nethermind Client, which powers roughly 30% of the network—Nethermind builds critical protocol upgrades and the foundations of leading Layer 2 ecosystems. The company's Blockchain-as-a-Service offering brings this proven engineering capability to institutional deployments, ensuring performance, security, and compliance at scale.

L2BEAT

L2BEAT is an independent, public goods research and transparency initiative focused on Ethereum's Layer 2 ecosystem, used by exchanges, custodians, funds, and infrastructure providers. L2BEAT provides standardized, plain-English disclosures on each L2's security guarantees and risks, tracks upgrades and incidents that may change those assumptions, and offers dashboards that let you compare those systems throughout various aspects: risk assessment, decentralization maturity, activity, total value secured, data availability, liveness, settlement costs.


ETHEREALIZE
NETHERMIND
L2BEAT


W3G®