Industry Analysis: Blockchain

Idea In Short

Blockchain infrastructure has moved past its experimental phase and into production settlement, asset tokenization and enterprise record-keeping, yet the economics remain concentrated in a handful of layers. Value accrues disproportionately to base-layer protocols with entrenched developer ecosystems, to the node infrastructure and staking intermediaries that sit between users and validators and to specialized compliance tooling that regulated buyers now require. Application builders and most layer-2 networks compete away their margins through fee wars and token subsidies. For executives evaluating entry, the decision is not whether to build a blockchain but where in the stack to sit: infrastructure and compliance tooling offer better economics than protocol launches or generic application development. Incumbents should defend developer mindshare and interoperability standards rather than chase transaction volume, since bargaining power is shifting toward institutional buyers who now dictate integration terms with the confidence that switching costs, while real, are no longer prohibitive.

Blockchain infrastructure sits at an uncomfortable but clarifying moment. The speculative frenzy that defined its first decade has receded and what remains is a smaller, more disciplined industry building settlement rails, tokenization platforms and verification infrastructure for institutions that care more about uptime and compliance than about ideology. This shift matters to executives because the technology has quietly moved from experimentation to procurement and procurement decisions now carry real budget, real vendor risk and real competitive consequence. Understanding where value concentrates in this stack and where bargaining power is moving, is a prerequisite for any board considering an investment, an acquisition, or a build decision in distributed ledger technology.

Industry at a glance

Blockchain, as an infrastructure and technology industry, covers the protocols, networks and platforms that let independent parties agree on a shared, tamper-resistant record without a single trusted intermediary. This definition excludes the trading of cryptocurrencies as an asset class, exchange operations and token speculation, all of which belong to the separate cryptocurrency and digital-assets industry. What falls inside the scope here includes layer-1 networks such as Ethereum, Solana and Bitcoin's settlement layer, layer-2 scaling networks that batch transactions before settling on a base chain, permissioned enterprise platforms such as Hyperledger Fabric and R3 Corda and the developer tooling, node infrastructure and identity and compliance middleware that make any of these usable in production.

Customers span three distinct categories, each with different economics. Business-to-business buyers, largely banks, asset managers, insurers and supply chain operators, use blockchain infrastructure for asset tokenization, trade finance documentation and provenance tracking and they pay through licensing, integration services and node-hosting fees. Business-to-consumer usage flows mostly through wallets and applications built on top of public networks, where consumers pay transaction fees denominated in the network's native token rather than direct subscription charges. Business-to-government usage remains smaller but growing, concentrated in central bank digital currency pilots, land registries and identity systems, where government agencies typically fund development through grants or direct procurement rather than usage-based fees.

The industry's revenue models diverge sharply by layer. Public layer-1 networks earn revenue through transaction fees paid to validators, a portion of which often accrues to a protocol treasury or gets burned to create scarcity for the native token. Layer-2 networks earn fees for batching and compressing transactions, then pay a portion back to the underlying layer-1 for security and data availability. Enterprise platform vendors earn through software licensing, professional services and managed-node hosting, which resembles conventional enterprise software economics far more than it resembles crypto-native tokenomics. Capital intensity varies by segment: validator and mining infrastructure requires meaningful upfront hardware and energy investment, while software and tooling businesses are comparatively asset-light. Labor intensity is high across the board because the talent pool for cryptographic engineering and distributed systems remains scarce relative to demand. Regulatory intensity has risen sharply, particularly around stablecoin issuance, securities classification and anti-money laundering compliance for node operators and it now shapes which networks institutional buyers are willing to touch.

Industry segmentation

The industry organizes into six segments, dimensioned primarily by position in the technology stack and by the openness of the network to unknown participants. Layer-1 public networks form the base layer, providing consensus, security and native settlement for networks such as Ethereum, Bitcoin and Solana; these networks compete on decentralization, security budget and developer ecosystem size rather than on raw throughput alone. Layer-2 scaling networks, including optimistic and zero-knowledge rollups, sit above layer-1 chains and inherit their security while offering cheaper and faster transaction processing, competing primarily on cost, latency and the size of the applications already deployed on them.

Permissioned enterprise platforms constitute a distinct segment aimed at consortiums of known, vetted participants who need shared record-keeping without full decentralization; Hyperledger Fabric, R3 Corda and enterprise-focused Ethereum variants dominate here, competing on integration with existing enterprise software and on governance flexibility. Developer tooling and infrastructure-as-a-service providers, such as node hosting and application programming interface access layers, form a fourth segment that abstracts away the operational complexity of running blockchain infrastructure directly, competing on reliability, latency and breadth of chain coverage.

Staking and validator services make up a fifth segment, where firms operate or delegate validator infrastructure on behalf of institutions and retail holders who want exposure to network rewards without running hardware themselves; this segment competes on yield optimization, security track record and regulatory registration. Finally, identity, compliance and interoperability middleware forms a sixth segment addressing the specific institutional requirement to prove provenance, satisfy anti-money laundering rules and move assets across otherwise incompatible networks, a segment growing quickly as tokenization moves from pilot to production.

Market structure

Porter's Five Forces reveal an industry where rivalry is intense at the application and layer-2 tiers but where genuine pricing power concentrates in a small number of base-layer protocols and specialized infrastructure providers. Buyer power has risen as institutional adoption matures and switching costs, while real, have fallen with better interoperability tooling. Supplier power sits with scarce engineering talent and with the cloud and chip vendors that underpin validator economics. New entrants face low technical barriers to forking code but very high barriers to acquiring developer mindshare and liquidity. Substitutes remain viable wherever trustless verification is not actually required by the use case.

Porter's Five Forces analysis of the blockchain infrastructure industry

Bargaining power of buyers

Buyers in this industry range from individual application developers choosing which chain to build on, to large financial institutions negotiating enterprise licensing terms for permissioned platforms. Developer buyers exercise meaningful power because switching a live application to a different chain, while costly, is achievable with modern cross-chain tooling and developers gravitate quickly toward whichever network offers the best combination of low fees, reliable uptime and active tooling support. This mobility forces networks to compete aggressively on grants, incentive programs and fee subsidies to retain builders, which compresses protocol-level margins even for networks with large user bases.

Institutional buyers, including banks and asset managers evaluating tokenization infrastructure, wield disproportionate power because their deal sizes are large and their compliance requirements narrow the viable vendor pool substantially. A bank evaluating a settlement platform typically has only a handful of credible options that meet regulatory, security and liquidity thresholds simultaneously, yet within that shortlist the bank can negotiate aggressively on price and customization given the vendors' hunger for flagship institutional references. This dynamic has pushed enterprise blockchain vendors toward bespoke integration work and away from standardized pricing, eroding scale economics that would otherwise favor the vendor.

Retail buyers, meanwhile, hold comparatively little individual power but collectively shape which networks accumulate liquidity and attention, since network effects reward whichever chain retail activity concentrates around. The net effect is a buyer landscape where power is bifurcated:

> small buyers are individually weak but collectively decisive for network effects, while large institutional buyers are individually powerful and can extract favorable terms precisely because vendors need their credibility as much as their revenue

Buyer type	Source of leverage	Typical concession extracted
Application developers	Low switching cost with cross-chain tooling	Fee subsidies and ecosystem grants
Institutional financial buyers	Large deal size, narrow compliant vendor pool	Bespoke integration and custom pricing
Retail token holders	Collective influence over liquidity and adoption	Yield incentives and governance rights
Government and public-sector buyers	Regulatory leverage over market access	Data residency and audit concessions

Bargaining power of buyers

Bargaining power of suppliers

The most consequential suppliers to this industry are not physical input providers but scarce categories of talent and infrastructure. Cryptographic and distributed-systems engineers remain in short supply relative to the number of protocols and platforms competing for their attention and this scarcity gives senior engineering talent significant leverage over compensation, often paid partly in tokens whose value depends on the very project they are building. Protocol foundations and enterprise vendors alike report that engineering talent acquisition, not capital, is frequently the binding constraint on their roadmap.

Cloud infrastructure and semiconductor suppliers hold meaningful power over the validator and mining economics that underpin network security. A small number of hyperscale cloud providers host a disproportionate share of validator nodes, which raises concentration risk that regulators and network architects increasingly flag as a systemic vulnerability and it also means these cloud providers can influence hosting costs across the industry through pricing changes. Node infrastructure providers such as those offering application programming interface access to blockchain data have themselves become suppliers with real power, since most applications depend on a small number of these providers rather than running their own infrastructure, creating a chokepoint that a provider outage or price increase can expose instantly.

Staking pool operators represent a newer but rapidly consolidating supplier category. As institutional capital flows into staked exposure through exchange-traded products and delegated staking services, a small number of large staking providers now influence a meaningful share of validator activity on major networks, a concentration that raises governance and censorship-resistance questions even as it lowers operational friction for buyers.

Supplier category	Concentration level	Primary leverage mechanism
Distributed-systems engineering talent	High scarcity, low substitutability	Compensation premiums and equity-like token grants
Cloud hosting for validator nodes	Concentrated among few hyperscale providers	Infrastructure pricing and uptime terms
Node and API infrastructure providers	Concentrated among handful of specialist firms	Data access reliability and rate limits
Staking pool and custody operators	Growing concentration via institutional inflows	Delegated validator influence over consensus

Bargaining power of suppliers

Rivalry among existing competitors

Rivalry is most visible and most destructive to margins, at the layer-2 and application tiers, where dozens of scaling networks compete for a finite pool of liquidity and developer attention. Consolidation has already begun: two optimistic rollup networks now account for the large majority of layer-2 liquidity, leaving a long tail of smaller networks fighting over a shrinking remainder.1 This consolidation reflects a broader pattern in the industry:

> technical differentiation erodes quickly once code is open source, so competitive advantage shifts to distribution, security track record and the depth of applications already committed to a given network

At the layer-1 level, rivalry looks different because switching an entire ecosystem of applications and liquidity to a competing base chain is far more disruptive than switching a single application between layer-2 networks. This raises effective switching costs and dampens rivalry intensity for the leading base-layer networks, even as newer entrants continue to launch with aggressive incentive programs to bootstrap activity. Enterprise permissioned platforms compete on a different axis entirely, emphasizing integration with legacy enterprise software, governance flexibility for consortiums and vendor support rather than decentralization purity, which means Hyperledger Fabric and R3 Corda rarely compete head to head with public layer-1 networks for the same buyer.

Price competition is unusually visible in this industry because transaction fees are public and easily compared, which pushes networks toward token-funded subsidies to keep fees artificially low during growth phases. This dynamic can mask the true unit economics of a network, since a chain subsidizing fees through token emissions is effectively selling below cost until emissions taper or usage reaches self-sustaining fee revenue.

Competitive dimension	Layer-2 networks	Layer-1 base networks
Primary competitive lever	Transaction cost and speed	Security budget and developer ecosystem
Switching cost for buyers	Moderate, falling with bridging tools	High, tied to liquidity and application lock-in
Consolidation trend	Rapid, concentrating around two leaders	Slower, dominated by incumbents
Margin sustainability	Weak absent fee-paying volume	Stronger where fee revenue is self-sustaining

Rivalry among existing competitors

Threat of new entrants

Technical barriers to entry are low in the narrow sense that blockchain protocol code is largely open source and can be forked and modified quickly, which explains why new layer-1 and layer-2 networks continue to launch regularly. But technical barriers are not the barriers that matter most in this industry. The real barriers are developer mindshare, liquidity depth and security track record, none of which a new entrant can simply copy from an incumbent's codebase. A forked protocol inherits none of the original network's applications, users, or accumulated trust, which is why most new chain launches struggle to gain meaningful traction despite technically credible engineering.

Capital requirements for launching a competitive layer-1 network have risen because credible security now requires either a large, well-distributed validator set or a substantial treasury to subsidize early adoption, both of which take significant capital and time to establish. New entrants targeting the enterprise permissioned segment face a different barrier:

> convincing conservative institutional buyers, particularly regulated financial institutions, to entrust critical infrastructure to an unproven vendor, a sales cycle that can stretch over years and favors incumbents with existing regulatory

relationships and reference clients

A newer category of entrant is emerging around regulated, purpose-built layer-1 networks backed by consortiums of established financial institutions, illustrated by a group of major European banks launching a jointly owned layer-1 network specifically for tokenized asset settlement.2 This type of entrant sidesteps the developer-mindshare barrier by bringing its own captive institutional demand, suggesting that future entry may increasingly come from consortiums with built-in customers rather than from independent startups competing purely on open technology.

Entry pathway	Barrier severity	Typical entrant profile
Fork an existing open-source protocol	Low technical, high adoption barrier	Independent development team or foundation
Launch a new layer-2 scaling network	Moderate, requires layer-1 partnership	Venture-backed infrastructure startup
Build a regulated consortium network	High capital, lower adoption barrier	Coalition of established financial institutions
Enter as enterprise tooling vendor	Moderate, requires sales credibility	Established enterprise software vendor

Threat of new entrants

Threat of substitutes

The most direct substitute for blockchain infrastructure is the conventional centralized database and it remains a genuine competitive threat wherever the specific properties of a blockchain, namely tamper resistance and multi-party trust without an intermediary, are not actually required by the use case. Many enterprise blockchain pilots that failed to reach production did so precisely because a shared database with careful access controls delivered the same practical outcome at a fraction of the operational complexity, a lesson the industry has absorbed slowly and expensively over the past several years.

Cloud-hosted shared ledger services, offered by major cloud providers as managed alternatives to running blockchain infrastructure directly, represent a softer substitute that captures some of blockchain's auditability benefits without its full decentralization overhead.

These services appeal particularly to enterprises that want tamper-evident record-keeping among known, trusted partners but have no need for permissionless participation or native token economics, effectively substituting away the parts of blockchain that are hardest to justify commercially.

Traditional financial clearing and settlement rails remain the dominant substitute in regulated finance and they retain significant advantages in legal certainty, established dispute-resolution mechanisms and regulatory familiarity that tokenized alternatives are still working to match. Substitution risk is lowest in use cases where trustless verification among mutually distrustful parties is the actual requirement, such as cross-border asset transfer among institutions with no pre-existing legal relationship and highest wherever participants already have contractual trust and simply need efficient record-keeping.

Substitute	Where it wins	Where blockchain still wins
Centralized enterprise database	Single-owner or tightly controlled data	Multi-party data with no trusted central owner
Cloud-managed shared ledger	Known-partner networks needing auditability	Permissionless participation and native settlement
Traditional clearing and settlement	Regulated domestic finance with legal certainty	Cross-border transfer among unrelated institutions
Paper and manual verification processes	Low-value, low-frequency transactions	High-value assets requiring provable provenance

Threat of substitutes

Value chain and profit pools

The blockchain value chain begins with protocol research and core development, the upstream stage where cryptographic primitives, consensus mechanisms and network architecture are designed and continuously improved. This stage is typically funded by foundations, venture capital, or grant programs rather than direct product revenue and it produces the open-source code that every downstream participant depends on without paying licensing fees for it directly.

The second stage, network operation and security provisioning, covers the validators, miners and staking infrastructure that actually run consensus and secure the ledger in exchange for block rewards and transaction fees. This is the most capital-intensive stage of the chain, requiring hardware, energy and increasingly, staked capital as collateral against misbehavior and it is where the industry's most direct analogy to traditional infrastructure operation exists.

Node infrastructure and data access forms a third stage, sitting between raw network operation and application development, where specialized providers abstract away the complexity of running and querying blockchain nodes directly. Developer tooling and smart contract platforms constitute the fourth stage, providing the programming environments, testing frameworks and security auditing services that let application builders ship products without reinventing cryptographic infrastructure from scratch.

The fifth stage, application and interface layer, is where end-user products actually live, spanning everything from decentralized finance protocols to supply chain tracking dashboards to tokenized asset marketplaces. Finally, compliance and identity middleware forms an increasingly important sixth stage that overlays the entire chain, providing the regulatory reporting, know-your-customer verification and cross-chain interoperability that institutional buyers now require before they will commit meaningful capital to any of the earlier stages.

Profit pool

Profit concentrates most heavily in two places that look superficially different but share a common characteristic: both convert a commodity input into a defensible, recurring relationship. Dominant layer-1 protocol ecosystems capture value through transaction fee revenue and treasury appreciation and because developer ecosystems and liquidity exhibit strong network effects, this value concentrates in a small number of networks rather than distributing evenly across the many chains that exist. The gap between the leading networks and the long tail has widened rather than narrowed as the industry has matured, contrary to early expectations that competition would erode any single network's advantage.

Node infrastructure and staking service providers occupy the second major profit pool, because they solve a genuine operational problem, namely the complexity of running reliable blockchain infrastructure, that most enterprises and even most application developers have no interest in solving internally. This segment behaves more like conventional infrastructure-as-a-service businesses, with subscription and usage-based revenue that is less exposed to token price volatility than protocol-level revenue.

Application-layer businesses, by contrast, have struggled to build durable profit pools. Open-source composability means a successful application's core mechanics can often be replicated by a competitor within weeks and fierce competition for liquidity and users has forced many applications to subsidize usage through token incentives rather than charge sustainable fees. Enterprise permissioned platform vendors sit in between:

> their profit pools are smaller than public network protocols but more stable, resembling traditional enterprise software licensing with multi-year contracts and high switching costs once a consortium has standardized on a platform

Industry economics and business models

Four business model patterns dominate the industry, each with distinct unit economics. The protocol-native model, used by public layer-1 and layer-2 networks, generates revenue through transaction fees paid in the network's native token, a portion of which typically funds a foundation or treasury while another portion rewards validators directly. This model resembles a two-sided platform in which validators and users must both be present in sufficient numbers for the network to function and it depends heavily on token economics design to balance inflation, security incentives and fee affordability simultaneously.

The infrastructure-as-a-service model, used by node hosting and staking providers, generates revenue through subscription fees or a percentage cut of staking rewards, more closely resembling conventional cloud infrastructure economics than crypto-native tokenomics. This model benefits from genuine economies of scale, since serving additional customers from existing node infrastructure carries low marginal cost once the fixed investment in reliable, geographically distributed infrastructure is made.

The enterprise licensing model, used by permissioned platform vendors such as those offering Hyperledger Fabric or Corda-based deployments, generates revenue through software licensing, implementation services and ongoing support contracts, structured much like traditional enterprise software sales with long sales cycles and high per-deal value. Finally, the application and protocol tooling model captures value through transaction fees on specific application usage, often supplemented by token issuance to bootstrap early growth, a pattern that has produced some durable businesses but many more that collapsed once token subsidies ran out and real fee revenue proved insufficient to sustain operations.

Cost drivers and scalability

Cost structure diverges sharply between the network operation stage and every other stage of the value chain. Validator and mining infrastructure carries substantial fixed costs in hardware and, for proof-of-work networks, energy, alongside variable costs tied to network activity and difficulty adjustments. Proof-of-stake networks, now dominant among major public chains, have shifted this cost structure meaningfully by replacing energy-intensive mining with capital staking, which lowers the ongoing operating cost of security but raises the capital commitment required to participate meaningfully.

Software and tooling businesses, by contrast, exhibit cost structures typical of digital infrastructure companies, dominated by engineering talent costs with comparatively low marginal cost per additional user once core platforms are built. This creates strong economies of scale for node infrastructure and developer tooling providers, since the cost of serving an additional application developer or enterprise client is a small fraction of the fixed cost invested in building reliable, secure infrastructure.

Unit economics in this industry hinge on a distinction that is easy to overlook amid token price volatility: the difference between revenue generated by real, fee-paying usage and revenue or apparent growth generated by token issuance and incentive programs. Networks and applications that rely heavily on token emissions to subsidize low fees or high staking yields are effectively running at a loss funded by dilution, a pattern sustainable only as long as new capital keeps flowing into the token itself. The flywheel that genuinely compounds in this industry links developer activity to liquidity to user adoption and back to developer activity, but that flywheel only becomes self-sustaining once transaction fee revenue, not token emissions, funds the majority of network security spending.

Moats, advantages and strategic levers

Network effects constitute the strongest and most durable moat in this industry, operating on two intertwined dimensions simultaneously. Developer network effects mean that a chain with more existing applications and tooling attracts more developers, since developers can build faster by composing existing infrastructure rather than starting from scratch. Liquidity network effects mean that a chain with deeper existing liquidity pools attracts more capital, since users prefer venues where they can transact at scale without significant price impact. These two effects reinforce each other, which is why leading networks have proven remarkably resilient against technically superior challengers that lack an established ecosystem.

Switching costs provide a secondary but meaningful moat, particularly for enterprise permissioned platforms where a consortium of institutions has already invested in integration, governance agreements and staff training around a specific platform. Unwinding that investment to switch vendors carries real organizational cost well beyond the technical migration itself, which gives incumbent enterprise vendors pricing power on renewal even when a competitor offers superior technology.

Security track record functions as a reputational moat unique to this industry, since a network or platform that has operated for years without a catastrophic breach earns institutional trust that a newer, unproven alternative cannot claim regardless of its technical merits. This moat compounds over time and explains part of why institutional buyers gravitate toward established networks even when fees are higher than newer alternatives. Regulatory positioning has emerged as a final and increasingly decisive moat, since networks and vendors that have proactively built compliance capabilities, particularly around anti-money laundering and securities classification, are becoming the only credible options for regulated institutional buyers as frameworks such as the European Union's Markets in Crypto-Assets regulation take full effect.3

Strategic levers

Executives evaluating entry or expansion in this industry have several concrete levers available and the right combination depends heavily on where in the value chain a firm intends to compete. Customer segment focus is the first lever:

> firms that concentrate on a narrow, high-friction institutional use case, such as trade finance documentation or securities settlement, tend to build defensible positions faster than firms attempting to serve every possible blockchain use case at once, since deep specialization builds compliance and integration expertise that generalists cannot easily match

Vertical integration versus partnering represents a second major decision. A firm can choose to build its own layer-1 or layer-2 network to control the full technology stack, accepting the substantial capital and adoption risk that entails, or it can partner with and build on top of an established network, sacrificing some control and differentiation in exchange for inheriting an existing developer ecosystem and security track record. The partnering path has generally proven more capital-efficient for firms whose core value proposition lies in the application or compliance layer rather than in protocol design itself.

Geographic and regulatory strategy forms a third lever, since blockchain infrastructure firms increasingly need to choose which regulatory jurisdictions to prioritize rather than assuming a single global approach will work. Firms that invest early in regulatory licensing within major markets such as the European Union gain a credibility advantage with institutional buyers that unlicensed competitors cannot quickly replicate. Ecosystem orchestration is a fourth lever available primarily to well-resourced incumbents:

> funding developer grants, sponsoring hackathons and subsidizing early adopters to seed a self-sustaining application ecosystem, an expensive strategy but one that has proven effective at establishing the developer network effects that ultimately determine long-term dominance

Structural risks, regulation and trends

Regulatory risk remains the most consequential structural risk facing this industry and it has intensified rather than eased as adoption has grown. The European Union's Markets in Crypto-Assets framework has created binding obligations for crypto-asset service providers and issuers of asset-referenced and electronic money tokens, with authorized issuers already operating across multiple member states and a hard deadline forcing previously unlicensed providers to obtain authorization or exit the market.4 Firms operating across jurisdictions face the added burden of reconciling incompatible national approaches, a compliance cost that scales poorly for smaller entrants and increasingly favors well-capitalized incumbents who can absorb legal and licensing overhead.

Technology disruption within the industry itself represents a second structural risk, particularly around the continued maturation of zero-knowledge proof systems, which are steadily reducing the computational and cost barriers to verifying transactions privately and efficiently. This shift threatens to reshuffle competitive positioning among layer-2 networks specifically, since zero-knowledge rollups offer stronger security guarantees than optimistic rollups and could displace incumbents that built their early advantage on the older architecture.

Geopolitical and supply chain risk affects the physical infrastructure layer of the industry, since semiconductor supply and energy availability both influence the cost and feasibility of validator and mining operations at scale and concentration of cloud hosting for validator infrastructure among a small number of hyperscale providers creates a systemic vulnerability that regulators have begun to scrutinize directly.

On the demand side, institutional tokenization has emerged as the clearest secular growth driver, with tokenized treasuries, money market funds, private credit and bank deposits moving from pilot programs into production deployment during the current cycle, following the money in a way that retail-driven speculation never sustainably did.[5] Supply chain verification represents a second durable demand driver, with luxury goods authentication, pharmaceutical serialization and food provenance tracking generating steady enterprise investment even as broader consortium platforms have struggled to scale.[6]

For entrants, the strategic playbook depends on ambition and capital availability. A niche entry strategy, targeting a specific institutional pain point with deep domain expertise, offers a faster path to sustainable revenue than a broad platform play, particularly for firms without the balance sheet to fund years of ecosystem subsidy. A partner-first approach, building compliance or application tooling on top of an established network rather than launching new infrastructure, minimizes capital risk while still capturing meaningful value if execution is strong. Regulatory strategy should be treated as a competitive weapon rather than a compliance afterthought, since early licensing in major jurisdictions increasingly determines which vendors institutional buyers will even consider.

Incumbents face a different set of choices centered on defending and deepening existing moats rather than chasing new territory. Defending developer ecosystem share requires sustained investment in tooling and grants even during periods when speculative attention has moved elsewhere, since developer migration, once it starts, is difficult to reverse. Expanding into adjacent institutional use cases, particularly tokenization infrastructure, allows established networks to capture new demand without diluting their core technical advantages. Deepening regulatory moats through proactive licensing and compliance investment positions incumbents to benefit disproportionately as frameworks such as the Markets in Crypto-Assets regulation narrow the field of credible institutional-grade options.

> The technology has quietly moved from experimentation to procurement and procurement decisions now carry real budget, real vendor risk and real competitive consequence

Caselet: Consensys and the infrastructure layer beneath Ethereum

Consensys, founded in 2014 by Ethereum co-founder Joseph Lubin, offers a clear illustration of how value has migrated within the blockchain stack over the past decade. The firm did not attempt to compete with Ethereum itself as a base-layer protocol, since Ethereum's own foundation and open-source community already controlled that layer. Instead, Consensys built a portfolio of businesses positioned squarely in the infrastructure and tooling stages of the value chain, betting that Ethereum's developer ecosystem would grow large enough to sustain a specialized services layer around it.

The firm's most consequential product, a node infrastructure and application programming interface access service, became one of the two or three dominant providers that most Ethereum application developers rely on to query blockchain data without running their own nodes. This positioning captured real economic value precisely because it solved a problem that almost every application developer faced but few wanted to solve internally, echoing the broader industry pattern in which infrastructure providers, not protocol founders, often capture the steadiest margins. Consensys also built MetaMask, a browser-based wallet that became the default entry point for a large share of Ethereum users interacting with decentralized applications, giving the firm a second strategic asset with strong distribution characteristics independent of any single application's success.

Consensys' history also illustrates the industry's characteristic volatility and the risk of overextension. During the period of intense speculative interest in blockchain applications, the firm expanded aggressively into dozens of internal ventures spanning decentralized finance, non-fungible tokens and enterprise consulting, many of which were later spun out, shut down, or consolidated as market enthusiasm cooled and capital discipline returned. This pattern of expansion followed by consolidation mirrors the broader application layer's struggle to convert technical novelty into durable, fee-paying business models, reinforcing the value chain analysis that infrastructure and tooling positions tend to outlast application-layer bets built on speculative attention.

The firm's regulatory posture has become an increasingly central part of its strategy, reflecting the industry-wide shift toward compliance as a competitive differentiator rather than a constraint. Consensys has engaged directly with regulators across multiple jurisdictions, including litigation over the classification of certain products under securities law, a posture that positions the firm to benefit from regulatory clarity even as the process of achieving that clarity has been contentious and costly. This willingness to engage rather than avoid regulatory scrutiny distinguishes firms likely to remain viable institutional partners from those that treated regulation as a problem to route around.

Consensys' trajectory demonstrates several principles that recur throughout this industry analysis. Positioning at the infrastructure and tooling stage of the value chain, rather than attempting to own the base protocol or chase every application opportunity, produced more durable revenue than speculative application bets. Owning a widely distributed access point, in this case a wallet used by millions of people as their default gateway to Ethereum, created a strategic asset with value independent of any single product cycle. And engaging proactively with regulatory scrutiny, rather than avoiding it, has positioned the firm more favorably as institutional buyers increasingly demand regulatory clarity before committing capital. Each of these lessons maps directly onto the value chain and moat analysis developed earlier in this article, making Consensys a useful reference point for executives evaluating where to position a new venture within blockchain infrastructure.

Closing perspective

The industry's next phase will likely reward discipline over experimentation. Firms that identify a specific, high-friction institutional problem, build durable infrastructure or compliance capability around it and invest early in regulatory credibility are positioned to capture disproportionate value as blockchain infrastructure continues its transition from speculative technology to procured utility. Firms still chasing broad platform ambitions without a clear fee-paying customer risk repeating a pattern the industry has already lived through once, funded by token emissions rather than by revenue that survives a downturn in market sentiment.

- 1layer-2 liquidity has consolidated around two dominant networks
- 2a consortium of major European banks launched a jointly owned layer-1 network for tokenized settlement
- 3the European Union's Markets in Crypto-Assets regulation reached full applicability for crypto-asset service providers in late 2024
- 4nineteen electronic money token issuers were authorized under the Markets in Crypto-Assets framework as of March 2026
- 5institutional tokenization is moving from pilot into production across tokenized treasuries, money market funds and private credit
- 6supply chain blockchain applications continue to expand across luxury authentication and pharmaceutical serialization

Summary

Blockchain infrastructure now functions as a specialized settlement and record layer sitting beneath tokenized finance, supply chain verification and cross-border payment rails, rather than as a wholesale replacement for enterprise databases. Its economics reward protocols and intermediaries that convert open code into defensible distribution: dominant layer-1 networks, the node operators and staking services that abstract away validator complexity and the compliance middleware that regulated institutions now require before they will touch a public chain. Application-layer competition remains brutal and margin-light. The strategic levers that matter most are developer ecosystem depth, interoperability positioning and regulatory readiness, each of which compounds over time in ways that raw transaction throughput does not. Executives should treat blockchain as an infrastructure procurement decision rather than a technology bet, weighing total integration cost against the narrowing set of networks that credibly combine security, liquidity and institutional trust.