SEPTEMBER 2025

BEYOND TRIBALISM AND TRANSPARENCY: THE CASE FOR A COLLABORATIVE CRYPTO FUTURE

COMMISSIONED BY midnight foundation

THEBLOCK.CO

ABSTRACT

Public blockchains have seen two fundamental structural barriers to widespread adoption. First, ideological tribalism has fragmented the ecosystem, splintering developer talent, liquidity, and community focus across competing "winner-take-all" networks rather than fostering collaborative innovation. This fragmentation has created an engineering tax that slows progress, with 2024 seeing the first net decline in new developer participation since 2019. Secondly, the inherent transparency in public blockchains has deterred enterprise adoption, as organizations often cannot expose sensitive commercial data, supplier relationships, or transaction volumes to competitors and regulators through immutable public ledgers.

The economic consequences of this fragmentation are substantial and measurable. Cross-chain bridge exploits have resulted in billions in losses, while the proliferation of Layer-1 and Layer-2 networks has scattered liquidity and forced developers to choose between ecosystems. However, market signals indicate a shift toward collaboration, with venture capital increasingly flowing toward multichain and privacy-focused projects. In 2024, funding for interoperability and privacy solutions grew 62% year-over-year, while multichain projects secured $780 million in funding, representing an 84% increase from the previous year.

This report examines how selective disclosure privacy combined with chain-agnostic design can resolve these adoption barriers, drawing parallels to the internet's evolution from fragmented networks to unified infrastructure through open standards and layered privacy protocols. Using Midnight's cooperative blockchain architecture as a case study, we explore how privacy-preserving interoperability can enable enterprises to leverage blockchain benefits while maintaining commercial confidentiality, potentially unlocking the industry's untapped addressable market through collaborative rather than competitive ecosystem development

COMMISSIONED BY midnight foundation

The Midnight Foundation is an organization dedicated to growing the Midnight network — a fourth-generation blockchain built for secure, compliant, and private decentralised applications — and supporting the global community around it. We help developers, creators, and privacy advocates build tools that protect personal data, support digital freedom, and power the breakthrough generation of blockchain innovation.

More about The Midnight Foundation: Website | LinkedIn | X

RESEARCHED BY THE BLOCK PRO · RESEARCH

The Block Pro is The Block's premium product portfolio designed to help institutions evaluate opportunities in digital assets. Pro's research, news, and data products are powered by teams of subject matter experts deeply entrenched in the digital asset ecosystem who deliver actionable intelligence so businesses can make informed decisions.

The Block Research produces research content covering the digital assets, fintech, and financial services industries.

CONTACT

Email: research@theblock.co X: @TheBlock__

ACKNOWLEDGMENTS

We would like to thank the Midnight Foundation for commissioning this research report. We would also like to thank everyone at The Block who assisted with this report - design team: Michael Elshahat; research team: Ivan Wu, Alessandro Angelucci, and Brandon Kae.

The authors of this report may hold tokens mentioned in this report. Please refer to The Block's financial disclosures page for author token holdings.

AUTHOR

Ivan Wu
Research Analyst
X | LinkedIn

Brandon Kae
Research Analyst
X

Alessandro Angelucci
Research Analyst
X | LinkedIn

TABLE OF CONTENTS

4 **ACKNOWLEDGEMENTS**
5 **TABLE OF CONTENTS**
6 **1. TRIBALISM AND TRANSPARENCY AS BARRIERS TO ADOPTION**
6 1.1 How Tribalism Became the Industry's Default Operating System
9 1.2 The Downside of Radical Transparency
9 1.3 Tracing the Economic Cost of Fragmentation
13 1.4 Why Collaboration Requires Selective Disclosure
14 **2.THE CASE FOR SECURE COLLABORATION**
14 2.1 How Open Standards and Layered Privacy Enabled Mass Adoption of the Internet
15 2.2 Why Collaboration Requires Selective Disclosure, Compliance-Grade Privacy, and...
16 2.3.0 The Rise of Layer-1 and Layer-2s
18 2.3.1 Multichain Single-Chain dApp Adoption
23 2.3.3 Growth in Multichain and Privacy-Focused Blockchain Investments
26 **3. MIDNIGHT'S COOPERATIVE DESIGN AND MULTI-PHASE TGE**
27 3.1 Compact Design
28 3.2 Composability
29 3.3 Use Cases
30 3.4 Timeline
32 **4. CONCLUSION: BREAKING DOWN THE BARRIERS TO MASS ADOPTION**

1. TRIBALISM AND TRANSPARENCY AS BARRIERS TO ADOPTION

A decade and a half after Bitcoin's genesis block, public blockchains still lag behind their expected adoption curve. Two structural frictions explain much of that shortfall.

First, ideological tribalism has splintered talent, liquidity and mindshare across competing, "winner-take-all" ecosystems. Second, sunlight-by-default transparency has limited adoption due to users' and corporations' fears and general unwillingness towards potential surveillance, commercial leakage and regulatory risk.

Unless the industry confronts both obstacles at once, the total addressable market for decentralized infrastructure will remain largely untapped. This report explores how selective-disclosure privacy and chain-agnostic design can resolve these barriers. We begin by quantifying the problem.

1.1 HOW TRIBALISM BECAME THE INDUSTRY'S DEFAULT OPERATING SYSTEM

Blockchain history is littered with zero-sum narratives. The 2017 Bitcoin block-size schism

is instructive. One camp argued for larger blocks to prioritize transactional throughput and everyday utility; the other insisted on smaller blocks to protect decentralization, make it easier for ordinary users to run full nodes, and safeguard the security assumptions of the network. In short, it was a debate about utility at the edge versus security at the core, and it set the template for how technical design questions would be reframed as existential identity conflicts for years to come.

For example, in the seven months spanning November 2024 to May 2025, Solana surpassed Ethereum in monthly fee revenue, prompting headlines that cast the narrative of a changing of the guard rather than a sign of healthy competition.

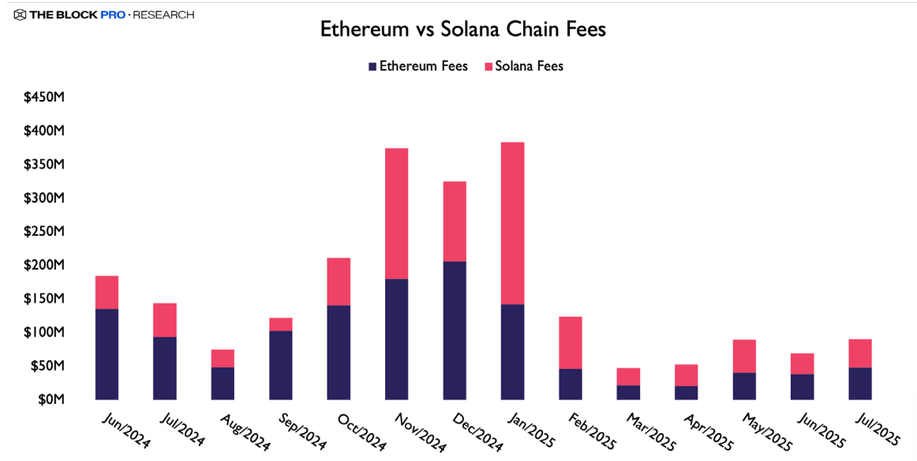

Figure 1: Fees generated by Ethereum and Solana blockchains Source: The Block

This was prevalent in social sentiment on X as well, where Solana's X account acquired more followers than Ethereum's X account in 38 out of the 42 weeks spanning June 2024 to March 2025. During this period, the latter acquired over 51K followers while the former

managed just 26K, showcasing a general theme of how sentiment for a project in the industry fluctuates alongside hype and excitement.

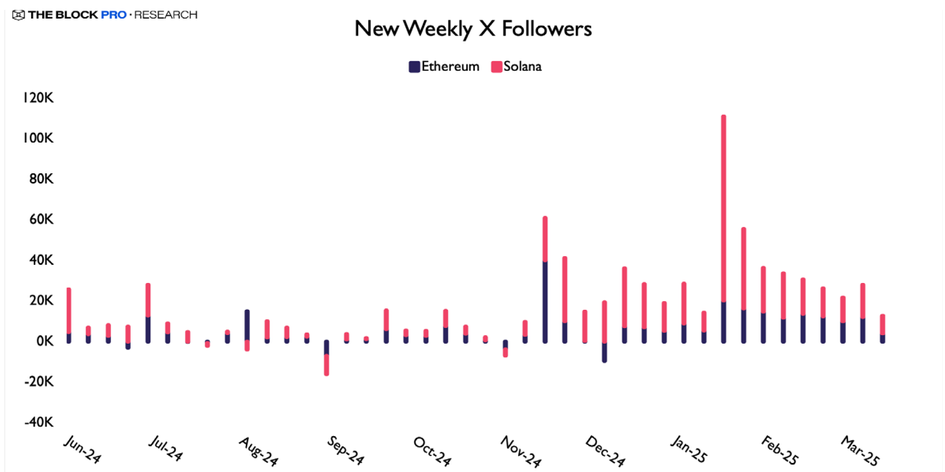

Figure 2: Weekly X Follower Change

Source: The Block

More recently, the 2025 theoretical throughput arms race between MegaETH and Monad, two blockchains that have yet to even launch their respective mainnets as of the time of writing, has pitted near-instant finality against monolithic security, drawing developers into mutually incompatible roadmaps instead of converging on shared standards. The parallel with the block-size debate is clear, where once again the field is being asked to choose between speed and feature-rich utility on the one hand and conservative security-first design on the other. Yet the outcome is arguably predictable: duplicated tooling, fragmented liquidity and adversarial marketing that confuses regulators and end-users alike. Developers devote disproportionate energy to deciding where to build instead of what to build.

1.2 THE DOWNSIDE OF RADICAL TRANSPARENCY

If tribalism fragments the ecosystem, transparency constrains its usefulness. The immutable public ledger still does exactly what it was designed to do, which is to deliver an open, verifiable state without trusted intermediaries, and that is valuable for many use cases. But the very properties that make public ledgers powerful also make them unsuitable for broad, institutional-grade adoption. Consumers do not want their financial lives trivially traceable, and enterprises cannot expose supplier lists, volumes, or margins to competitors, or run afoul of data-protection regimes, every time they settle a transaction. The upshot is not that public chains are "wrong," but that they are not for everyone. They excel where transparency is a feature; they fall short where selective confidentiality is a requirement. The Midnight litepaper observes that developers face "decision fatigue regarding the best ways to manage the volumes of data," while customers demand stronger control and businesses shoulder growing liability from leaks and breaches. Sentiment data corroborates the shift, with a March 2024 analysis from Deloitte stating how global media signals show that only 32% of coverage is positive, with crime, compliance and ethics dominating the negative cohort.

For privacy-sensitive sectors such as healthcare, supply-chain and financial services, the prospect of exposing transaction graphs that reveal counterparties, volumes, or margins is commercially untenable. Large enterprises, therefore, confine blockchain pilots to tightly permissioned testbeds or abandon them altogether.

1.3 TRACING THE ECONOMIC COST OF FRAGMENTATION

The economic drag created by tribalism and radical transparency becomes evident when one follows the chain of cause and effect that begins with developer behavior and ends with capital loss. As of the end of Q2 2025, approximately 25% of open-source crypto engineers or "developers" contribute code to several blockchains at once, a practice that looks collaborative on the surface but in reality dilutes expertise and slows release velocity.

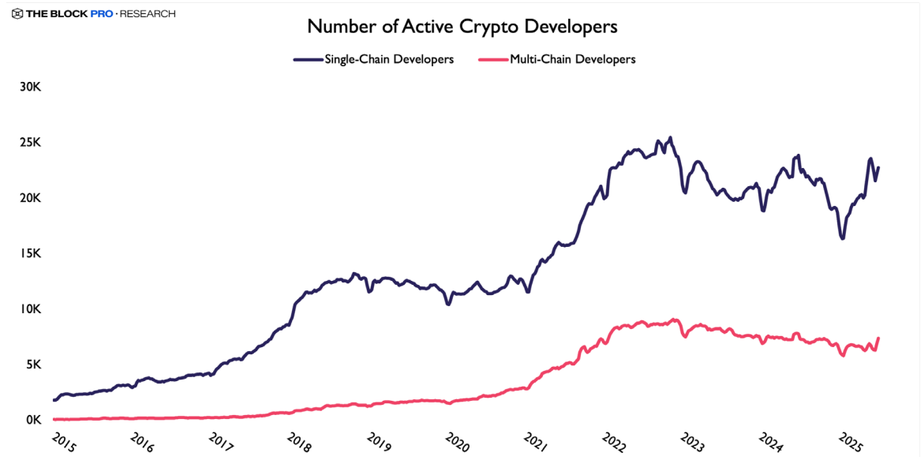

Figure 3: Number of developers active on single vs multiple chains Source: Crypto Ecosystems, as of 30 June 2025

Instead of compounding knowledge inside an interoperable stack, the community is forced to reinvent wallets, bridges and tooling for every major chain. The result is an engineering tax that reduces the pace of meaningful innovation. That tax has already discouraged new entrants, with 2024 seeing a -15% year-over-year (YoY) decline in first-time contributors or "developers", the first net yearly contraction of this metric since the prior "bear market" in 2019. Put simply, the harder it is for a newcomer to decide which camp to join, or to master several at once, the more likely that newcomer is to stay on the sidelines.

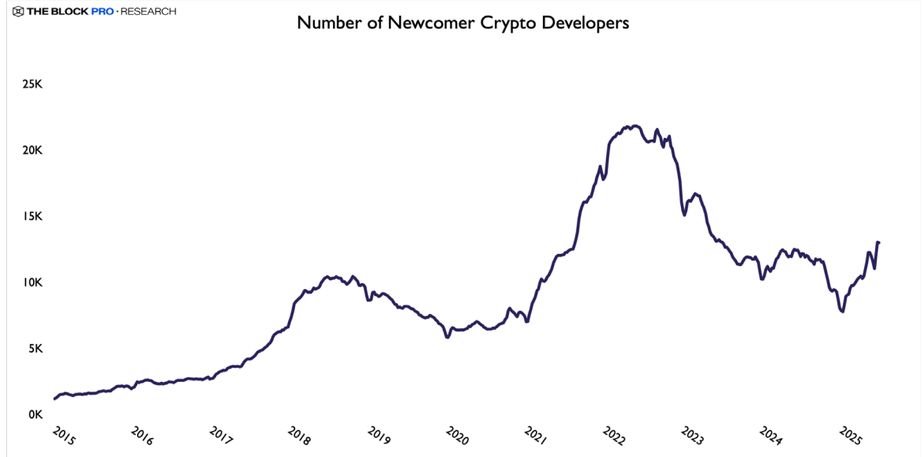

Figure 4: Number of new developers in crypto Source: Crypto Ecosystems, as of 30 June 2025

Scarce engineering resources, in turn, give rise to a patchwork liquidity architecture. Because assets are native to siloed chains, value must cross those silos through bridges or wrapped tokens. Every bridge represents duplicated functionality that exists only because the underlying networks refuse to interoperate at the base layer. Worse, each bridge expands the attack surface.

Exploits against cross-chain bridges erode user trust and draw regulatory scrutiny. Chainalysis estimated ~$2B stolen from cross-chain bridges in 2022, back when the multi-chain narrative was in its nascency. These breaches were arguably predictable costs of maintaining redundant infrastructure in a fragmented ecosystem. This matters enormously for institutions. Risk officers and boards, already cautious about novel infrastructure, see billion-dollar losses, rising compliance scrutiny and unclear legal liability, and conclude that the technology is not yet fit for mission-critical workflows. That conclusion withholds not just capital, but also the steady demand and integration work that make ecosystems durable.

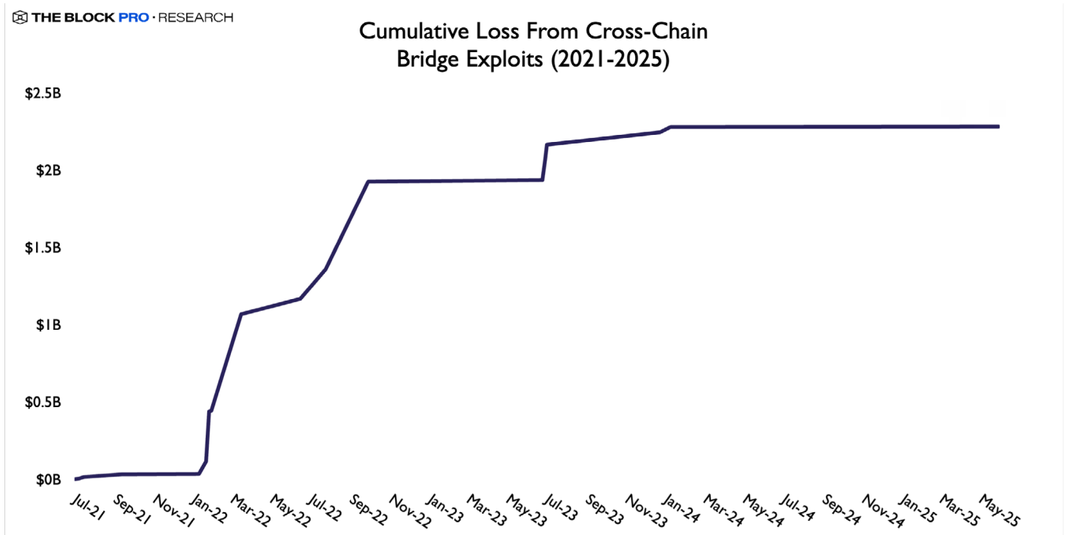

Figure 5: Cum. value lost to bridge exploits Source: The Block, as of 30 June 2025

Once capital is lost or withheld, liquidity retreats to whichever chain appears safest, yields compress, and ecosystem treasuries and venture pipelines tighten. Grants and hackathons become scarcer while conference travel stipends and training budgets are cut. The human toll is easy to miss in the charts but obvious on the ground: young engineers testing a first career bet, Web2 developers spending scarce professional-development funds to attend a hackathon, independent researchers trying to publish without a sponsor. When roadmaps stretch and funding windows shrink, these builders face hard choices about staying in the field or returning to steadier paths.

That attrition feeds back into the core problem. Fewer fresh builders means slower iteration and more reliance on brittle bridges. Each exploit or compliance incident then damages confidence, which further narrows funding, which further discourages newcomers. The data points of developer dilution, declining new-developer growth, bridge losses and institutional caution are thus not isolated statistics but sequential links in a single causal chain. The cycle is self-reinforcing until a coordination layer reduces switching costs for developers and allows value to move privately and natively across chains.

1.4 WHY COLLABORATION REQUIRES SELECTIVE DISCLOSURE

The internet achieved scale only after heterogeneous networks converged on open standards such as TCP/IP and then layered confidentiality through protocols like TLS. Public blockchains have mastered openness but not confidentiality. Tribal maximalism repels everyday users, and radical transparency deters enterprises, so the logical progression is an interoperable coordination layer that embeds granular, compliance-grade privacy.

Section 2 will examine how open standards combined with selective disclosure enable secure collaboration across chains, while Section 3 will demonstrate how Midnight's multi-ecosystem Token Generation Event and Halo2-powered architecture provide an early blueprint for that future.

2. THE CASE FOR SECURE COLLABORATION

2.1 HOW OPEN STANDARDS AND LAYERED PRIVACY ENABLED MASS ADOPTION OF THE INTERNET

The internet's transformation from isolated research networks to a unified global infrastructure provides a relevant framework for understanding how technical cooperation can overcome adoption barriers. The transition from ARPANET's restricted access model to TCP/IP's open standard, later enhanced by TLS encryption, demonstrates that widespread adoption occurs when protocols enable both interoperability and selective privacy controls.

The internet's path demonstrates how collaborative standards can overcome early adoption barriers without compromising security or functionality. ARPANET's initial design served a limited academic and research community, constrained by closed protocols and restricted access controls. The development of TCP/IP as an open standard marked a fundamental shift toward interoperability, enabling diverse networks to communicate seamlessly regardless of their underlying infrastructure. This protocol standardization created the foundation for exponential growth by removing technical barriers that

previously fragmented early computer networks.

The subsequent introduction of Transport Layer Security represented a critical evolution in internet architecture. TLS enabled selective privacy by allowing secure communications while maintaining the open nature of underlying protocols. The combination of open interoperability standards with robust privacy mechanisms addressed two seemingly contradictory requirements: broad accessibility and selective confidentiality. This architectural approach enabled the internet to support both public information sharing and private commercial transactions within the same infrastructure framework.

2.2 WHY COLLABORATION REQUIRES SELECTIVE DISCLOSURE, COMPLIANCE-GRADE PRIVACY, AND CHAIN-AGNOSTIC DESIGN

Current blockchain infrastructure reflects the pre-standardization internet era, where incompatible networks limited utility and growth potential. However, emerging protocols seem to be embracing multichain collaboration to achieve superior performance metrics compared to single-chain alternatives. Private markets have shown shifting capital allocation patterns, where investors increasingly look to allocate to projects that facilitate chain-agnostic functionality and privacy-preserving collaboration.

Compliance-grade privacy represents a fundamental requirement for institutional participation in blockchain ecosystems. Organizations operating in regulated industries require assurance that their blockchain activities can meet existing privacy standards and audit requirements. This necessity extends beyond simple data protection to encompass transaction privacy, participant anonymity when required, and the ability to demonstrate compliance without revealing underlying business information. Current blockchain implementations that lack these privacy controls effectively exclude significant portions of the traditional economy from participating in decentralized systems. Paul Brody from EY emphasizes this point, “The number one issue for enterprise users and for more serious institutional investors, is privacy. Blockchains don't natively have privacy,” and

"businesses don't want to disclose all the details of the contracts. ... They are very happy to tell you how many tons of carbon they save — they just don't want you to be able to see that on a week-to-week or a day-to-day basis."

The market's evolution toward collaborative blockchain infrastructure addresses fundamental limitations that have constrained institutional adoption and enterprise integration. Selective disclosure mechanisms, compliance-grade privacy features, and interoperable design principles represent essential components for protocols seeking to bridge the gap between blockchain's technical capabilities and real-world application requirements. The convergence of these factors suggests that the industry is approaching a critical juncture where collaborative approaches may define the next phase of blockchain development and adoption.

2.3.0 THE RISE OF LAYER-1 AND LAYER-2S

The rapid expansion of both Layer-1 and Layer-2 networks has created a more diverse, but also more fragmented blockchain ecosystem. The cumulative number of Layer-1s increased steadily through the 2010s, reaching a plateau around 2023 as competition matured. At the same time, the proliferation of Layer-2s since 2020 has added another layer of complexity to the landscape. While this growth reflects innovation and scalability progress, it has also splintered liquidity and fractured communities across multiple execution environments.

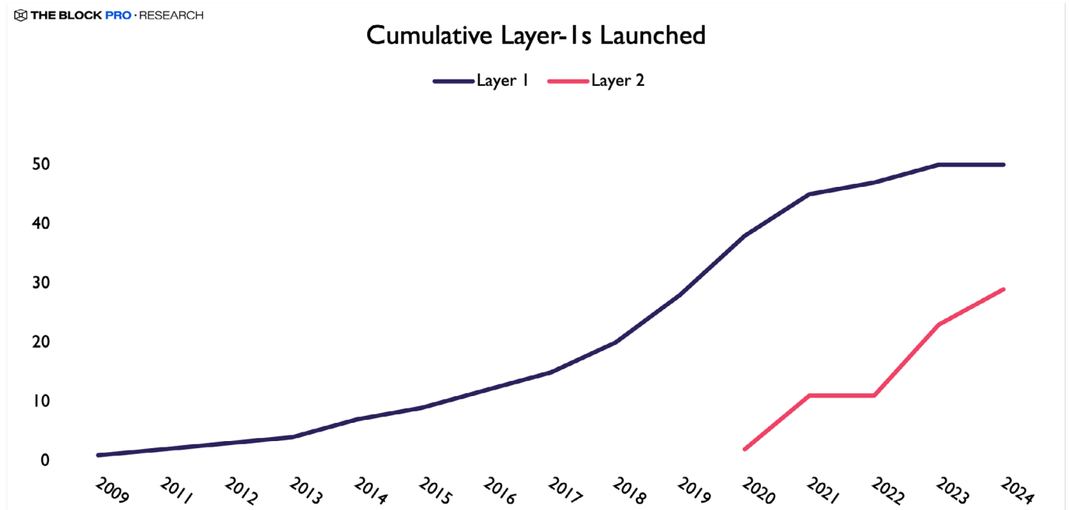

Figure 6: Cumulative number of L1 and L2 chains laucnhed Source: The Block

This proliferation of chains has introduced liquidity fragmentation, where capital and user activity are dispersed across numerous isolated pools. Instead of deep liquidity concentrated on a handful of platforms, trading volume, DeFi collateral, and governance participation are now scattered across dozens of Layer-1 and Layer-2 ecosystems. Fragmented liquidity reduces efficiency, raises slippage costs, and complicates institutional deployment, as capital allocation must be carefully managed across heterogeneous networks with different technical, economic, and security models.

The multiplication of ecosystems has also given rise to tribalism within the industry. Each chain seeks to establish its own developer community, cultural identity, and narrative, often leading to competition rather than collaboration. This tribalism manifests in fragmented developer resources, mutually exclusive governance systems, and user loyalty that prioritizes one network's success at the expense of broader ecosystem interoperability.

The result is an environment where innovation is abundant but siloed, creating barriers to collaboration and slowing the development of unified standards that could accelerate mainstream adoption.

While the diversity of chains fosters experimentation and scalability, it also intensifies fragmentation and tribalism that impede the very interoperability and collaborative infrastructure required for institutional adoption. This dynamic makes the case for multichain solutions, interoperability standards, and privacy-preserving collaboration even more urgent.

2.3.1 MULTICHAIN SINGLE-CHAIN DAPP ADOPTION

An analysis of the top 30 protocols by total value locked (TVL) reveals the current deployment preferences among leading DeFi applications. Of the 30 projects, 13 operate on a single chain, while 17 are deployed on two or more. Sixteen protocols operate within EVM-compatible environments, including Ethereum mainnet and its layer-2 solutions, while four protocols maintain deployments specifically on Ethereum mainnet. Six protocols have chosen single-chain deployments on non-Ethereum networks, three protocols operate within the Solana ecosystem, and one protocol maintains mixed virtual machine deployments across both Ethereum and Solana environments. This distribution underscores the dominance of EVM architecture in capturing institutional and retail capital, showcasing the preference for multichain strategies.

Figure 7: Top protocols by which chain they are on Source: DeFiLlama

The concentration of protocols within EVM and single-chain environments reflects several practical considerations faced by many projects. Development complexity increases significantly when maintaining codebases across different virtual machine architectures, requiring specialized expertise and duplicated security auditing processes. Liquidity fragmentation represents another critical concern, as spreading TVL across multiple chains can reduce capital efficiency and trading depth on individual networks. Additionally, governance coordination becomes more challenging when protocols must manage cross-chain operations, token distributions, and community engagement across disparate ecosystems.

Ethereum's continued dominance becomes more apparent when examining TVL

distribution across blockchain networks. Ethereum maintains approximately 62% of total value locked across all chains as of May 2025, demonstrating sustained capital preference for the network despite higher transaction costs. However, this concentration is beginning to shift as infrastructure improvements and enhanced interoperability solutions reduce barriers to cross-chain deployment. The "Others" category has expanded significantly since 2021, driven primarily by adoption on Binance Smart Chain, Bitcoin, Base, and TRON, indicating growing liquidity diversification across multiple networks. Solana has also established itself as a legitimate alternative ecosystem, capturing meaningful TVL beyond speculative token trading and demonstrating sustained protocol development and user adoption.

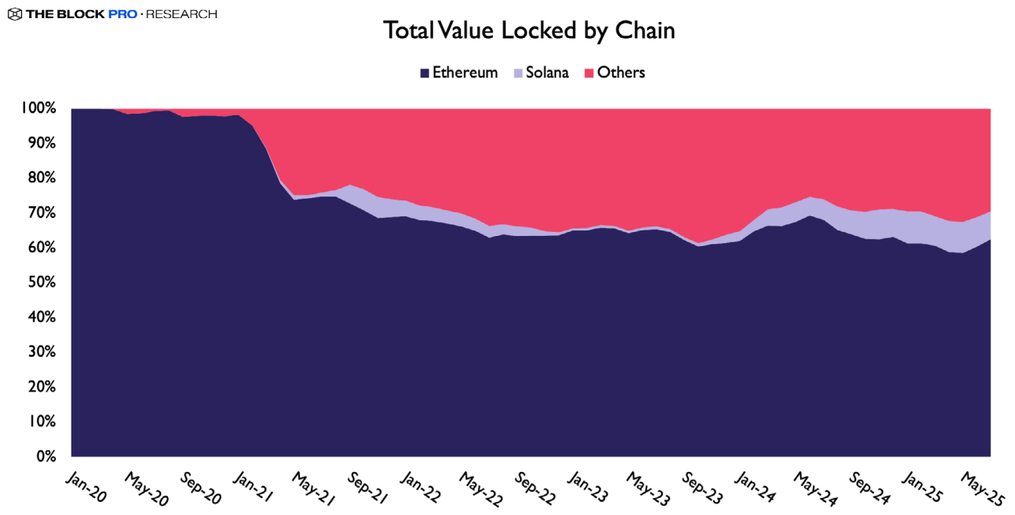

Figure 8: Total value locked on each blockchain

Source: The Block

As liquidity deepens across multiple chains and deployment tooling becomes more sophisticated, the current single-chain concentration among top protocols may transition to a multichain future. Enhanced bridging infrastructure, standardized development frameworks, and improved security protocols are reducing the technical friction that previously constrained multichain expansion. The emergence of privacy-preserving interoperability solutions further addresses enterprise concerns about cross-chain transparency, potentially accelerating institutional adoption of multichain strategies. These developments suggest that future protocol success may increasingly depend on the ability to capture value across diverse blockchain ecosystems rather than optimizing for single-chain dominance.

The strategic implications of multichain deployment present both opportunities and risks, as demonstrated by contrasting experiences in the DEX aggregator space. 1inch's expansion to Solana resulted in its market share rising from 58% at the beginning of May to 66% by the end of the month, illustrating how cross-chain functionality can rapidly expand user bases and transaction volumes. May's trade volume increased by ~260% MoM compared to April, and then by another 15% in June. 1inch total trade volume in the 2 months post-Solana expansion was higher than the previous 5 months combined. The protocol's ability to process transactions across both Ethereum and Solana environments provided users with expanded routing options and potentially lower transaction costs, driving increased adoption and market penetration.

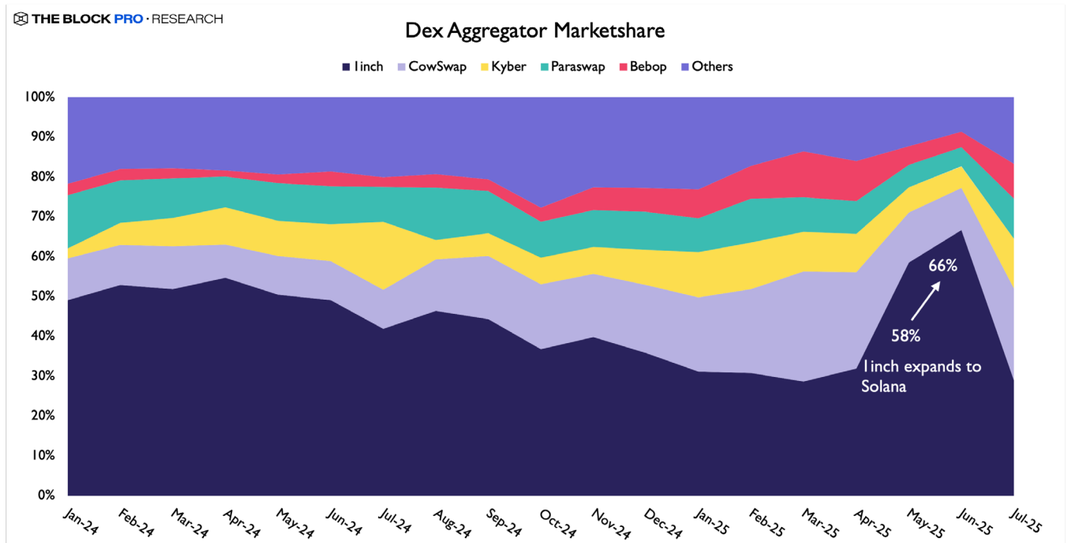

Figure 9: Marketshare of decentralized exchange aggregators Source: The Block

However, multichain deployment does not guarantee sustainable success, as evidenced by Lido's experience on Solana. Despite Solana's technical capabilities and growing ecosystem, Lido's stSOL service became financially unsustainable due to insufficient revenue generation relative to operational costs. The P2P Validator team reported spending approximately $700,000 while earning only $220,000, resulting in a net loss of $484,000 over the deployment period. In September 2023, the team requested $1.5 million over 12 months to continue operations, but a DAO vote in October 2023 resulted in over 92% of LDO token holders choosing to sunset the Solana service rather than subsidize continued losses. Lido's withdrawal highlights how low-fee structures, limited market share, and rising operational costs can undermine the financial viability of multichain operations, even on technically robust networks.

These contrasting outcomes suggest that successful multichain deployment requires careful evaluation of target network characteristics, revenue potential, and operational complexity. Protocols considering expansion must assess whether cross-chain deployment addresses genuine user demand or merely distributes existing liquidity across additional

networks without creating incremental value.

2.3.3 GROWTH IN MULTICHAIN AND PRIVACY-FOCUSED BLOCKCHAIN INVESTMENTS

Venture capital allocation patterns demonstrate a shift toward projects working towards a multichain future, including interoperability and privacy-preserving technologies. Deal count data for projects specifically focused on bridge/interoperability and privacy solutions reached 68 transactions in 2024, representing a 62% increase from the 42 deals recorded in 2023. This growth trajectory continues into 2025, with 21 deals already completed, positioning the year for another robust funding cycle despite broader market consolidation toward larger, later-stage rounds.

The projects attracting this specialized investment focus on addressing critical infrastructure gaps that have limited blockchain adoption. These solutions span fragmented liquidity management, zero-knowledge technology implementation, and cross-chain communication protocols. The consistent growth in this sector reflects investor recognition that interoperability and privacy represent fundamental requirements for blockchain infrastructure maturation rather than supplementary features.

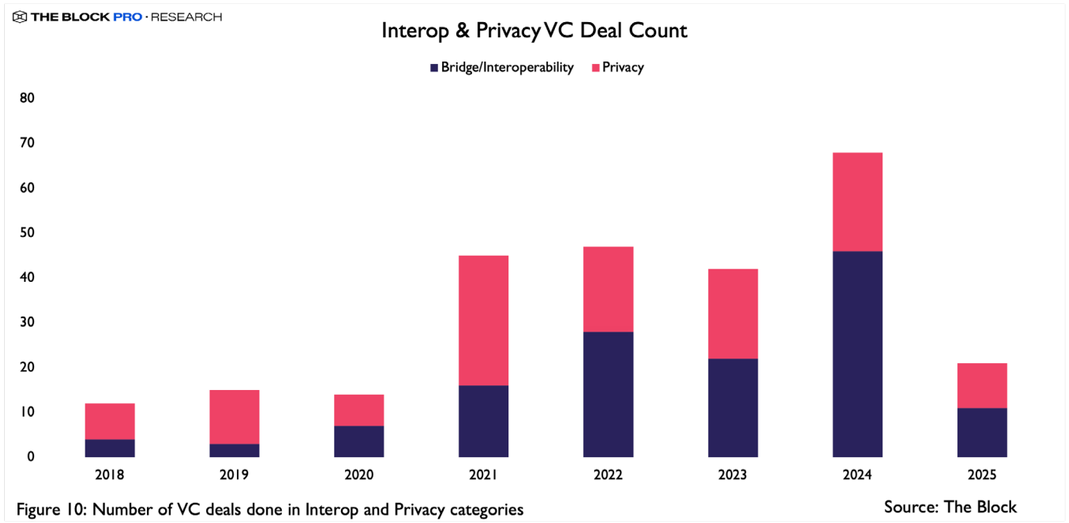

Figure 10: Number of VC deals done in Interop and Privacy categories

Source: The Block

Multichain project funding presents an even more compelling growth narrative, with projects operating across multiple blockchain networks securing significantly increased capital commitments. Total funding for multichain projects reached $780 million in 2024, up from $425 million in 2023, representing an 84% increase in capital allocation to these ventures. The deal count data shows sustained activity with nearly 200 transactions already completed in 2025, maintaining the momentum established over the previous year's 780 deals.

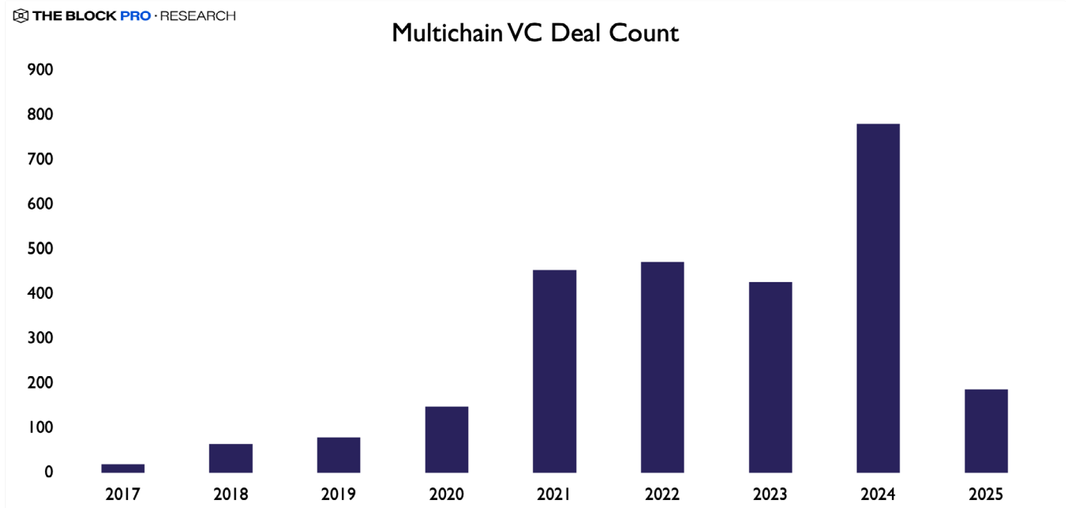

Figure 11: Number of VC deals done where venture operates on multiple chains

Source: The Block

The expansion of multichain development reflects several technological and market developments that have reduced barriers to cross-chain deployment. Improved bridging infrastructure, standardized development frameworks, and enhanced security protocols have enabled projects to deploy across multiple networks more efficiently than previous development cycles allowed. This includes both true multichain architectures that leverage distinct blockchain capabilities and projects deployed across multiple EVM-compatible chains to access different user bases and liquidity pools.

3. MIDNIGHT'S COOPERATIVE DESIGN AND MULTI-PHASE TGE

Midnight is a privacy-enhancing blockchain built in an attempt to address the frictions of tribalism and transparency discussed earlier in this report. By combining a cooperative, multichain economic model with a privacy-preserving smart contract framework, it seeks to boost blockchain adoption through privacy-as-a-service and seamless cross-chain interoperability.

At its core, Midnight's token economy runs on a dual-component system that separates value from utility:

- NIGHT is a fixed-supply governance and staking token that stores value while generating DUST.
- DUST is a non-transferable, shielded resource that powers private transactions and smart contract interactions. It is passively generated by NIGHT holders, decays if unused, and is burned when spent, keeping fee-related metadata such as transaction costs and originating addresses fully private.

This design mitigates fee volatility and MEV risks while supporting regulatory standards and exchange-listing requirements. Although DUST is non-transferable, Midnight enables an open-access "Capacity Marketplace" where NIGHT holders can lease and sponsor DUST for both Midnight users and external participants. This aligns network incentives and broadens access through off-chain brokers or dApps that facilitate sponsorship and smart contracts that automate leasing. The marketplace extends to "Babel Stations," which allow users to abstract DUST entirely by paying fees in other tokens or fiat. Babel Stations also provide a revenue stream for the treasury, supplying it with non-native assets such as ETH and USDC in addition to the NIGHT it receives from block rewards and unclaimed TGE tokens. This diversification blurs siloed economies in favor of interoperable collaboration and enables multichain grant programs to support ecosystem growth.

3.1 COMPACT DESIGN

While these cooperative economics ensure sustainable incentives, Midnight's novel smart contract framework enables decentralized applications that combine data protection with seamless interoperability. By integrating ZK-SNARKs and selective disclosure capabilities, Midnight allows users to decide exactly what information to reveal and to whom, without compromising verifiability or composability.

To accomplish this, Midnight has introduced Compact, a TypeScript-inspired programming language designed to offer a familiar coding experience while abstracting ZK complexities. Compact allows developers to focus on contract logic while explicitly defining private "witness" variables and ZK circuits to encode the rules of execution. Contracts then pass through Compact's compiler, which generates a custom TypeScript API for dApp interactions and circuit definitions for proof generation and verification.

Compact is built on Kachina, Midnight's private smart contract execution model. Kachina enables off-chain execution with public, on-chain verification. This lets users run contracts locally while only submitting proof of correct execution and the declared public state

to the network, ensuring auditability and compliance while keeping confidential details shielded.

3.2 COMPOSABILITY

Underpinning Midnight's execution is a robust cryptographic foundation inspired by the Halo2 proof system. Halo2 provides succinct, recursive proofs that are well-suited for interactive applications, while BLS12-381 curves enhance compatibility with major chains like Cardano and Ethereum. In addition, Midnight's Halo2 implementation has been designed with the capability to upgrade seamlessly to more advanced proof systems as industry standards evolve. As a result, Midnight can operate both as a standalone Layer 1 and as a plug-in privacy layer for other networks, allowing applications to access private execution without relocating from their native chains. This dual role prevents the fragmentation of users, developers, and liquidity across ecosystems and supports fee abstraction across multiple networks.

To further support interoperability, Midnight integrates widely adopted Ethereum standards through partnerships with OpenZeppelin and Zoniqx. These cover key token interfaces like ERC-20, ERC-721, ERC-1155, and ERC-7518, enabling developers to port or extend Ethereum-based applications to Midnight without abandoning their established tooling or redeveloping contracts entirely. This lowers switching costs and entry barriers, making it easier for existing projects to expand into Midnight's privacy-preserving environment.

Together, these capabilities create a platform suitable for both consumer and enterprise adoption, offering built-in privacy guarantees while ensuring scalability, security, and trustlessness. This facilitates previously impractical use cases, particularly in highly regulated or sensitive sectors.

3.3 USE CASES

USE CASE 1: IDENTITY & IDENTITY SERVICES

By acting as an open-access data protection platform, Midnight can enable a foundational rethinking of on-chain identity. Users could undergo a one-off traditional identity verification process, receive a ZK proof of verification, and reuse that proof for future attestations without disclosing more information than is strictly necessary. This capability could extend to a range of identity-centric services, ensuring regulatory compliance where required while preserving user privacy. For example:

- Proving eligibility to participate in on-chain governance without revealing identity or voting choices
- Demonstrating creditworthiness to a financial institution without exposing a complete financial history or unrelated sensitive data
- Meeting entry requirements for regulated or gated services without sharing personal identifiers

USE CASE 2: ENTERPRISE DATA & OPERATIONS

Midnight's selective disclosure capabilities could allow enterprises to leverage blockchain's benefits without exposing sensitive operational data. Enterprises could shield private client lists, proprietary processes, and internal transaction records while making verifiable proofs of compliance, solvency, or performance publicly accessible when required. This could extend to advanced financial applications, including private institutional DeFi and the tokenization of real-world assets like real estate, private equity, carbon credits, and insurance products. For example:

- Issuing bonds or equity on-chain while meeting all regulatory disclosure requirements without revealing investor identities or contractual details

- Tokenizing funds or alternative investments with built-in compliance checks and jurisdictional controls, without disclosing portfolio composition
- Verifying product provenance and regulatory conformity in supply chains without revealing supplier identities or commercial arrangements

3.4 TIMELINE

To realize these use cases at scale, Midnight's Token Generation Event is structured to maximize cross-ecosystem participation and long-term alignment. It represents a notable departure from traditional launches, distributing 100% of the NIGHT supply through three permissionless, cross-community phases:

PHASE 1: GLACIER DROP - CLAIM

- A broad token distribution targeting users across eight major blockchain ecosystems: Cardano, Bitcoin, Ethereum, Solana, XRPL, BNB, Avalanche, and Brave.
- Eligibility: Over $100 in native tokens held as of June 11, 2025; no OFAC-sanctioned addresses.
- Allocation: 50% to Cardano, 20% to Bitcoin, and the remaining 30% distributed proportionally among the other six ecosystems according to their market cap as of the snapshot.
- Claim process: Users prove wallet ownership and submit a new Cardano address; no KYC or fees beyond network costs.
- Thawing schedule: Claimed tokens unlock in four 25% tranches over 360 days, with the timing of tranches randomized on a per-user basis.
- Unclaimed tokens are split between the remaining TGE phases, commercial partnerships, liquidity provisions, and core network constituents such as the Midnight Foundation, the block reward reserve, and the on-chain treasury.

PHASE 2: GLACIER DROP - SCAVENGER MINE

- A 30-day period where unclaimed Glacier Drop tokens are distributed through an open, gamified challenge system.
- Mechanism: Users solve computational puzzles, with a new pool of NIGHT released daily. The process is designed to be accessible to the general public without requiring specialized mining software.
- Thawing: Same schedule as the Glacier Drop.

PHASE 3: GLACIER DROP - LOST-AND-FOUND

- A four-year window for eligible users to recover unclaimed Glacier Drop allocations.
- Claim process: Prove wallet ownership via smart contract (no claim UI provided).
- Thawing: Tokens are immediately liquid, but claimable amounts decay over time to incentivize early participation.
- Remaining unclaimed tokens after four years are sent to the treasury.

4. CONCLUSION: BREAKING DOWN THE BARRIERS TO MASS ADOPTION

The crypto industry is reaching an inflection point where continued growth may require structural advancements to reduce user friction. The analysis presented suggests that tribal maximalism and transparency limitations have created barriers for potential users who might otherwise participate in blockchain ecosystems. Conversely, projects aiming to move into a multichain environment have been rewarded through funding and usage growth.

The economic effects of ecosystem fragmentation extend beyond market inefficiencies. When engineering talent disperses across incompatible architectures, development velocity tends to slow and security auditing becomes duplicative. This contributes to infrastructure vulnerabilities, as demonstrated by various bridge exploits that have impacted user confidence and regulatory perception. These issues can create cycles where reduced trust leads to capital reallocation, potentially limiting developer resources and perpetuating coordination challenges.

Similarly, the transparency characteristics that distinguish blockchain technology may present obstacles for enterprise adoption. Organizations in regulated industries often require greater control over transaction visibility, counterparty disclosure, and commercial information exposure than current public blockchain implementations typically provide.

Midnight's design addresses these coordination challenges through cooperative mechanisms. The dual-resource model separates token value storage from network utility, while the selective disclosure framework allows participants to control information exposure without compromising verifiability. This could create conditions where enterprises can leverage blockchain infrastructure while maintaining commercial confidentiality, transactional cost predictability, and regulatory compliance. The multi-ecosystem Token Generation Event reflects this cooperative approach by distributing tokens across eight major blockchain networks rather than concentrating within a single ecosystem. This strategy suggests recognition that sustainable adoption may require building connections between communities rather than deepening divisions.