NETHERMIND

August 2026

REPORT

Assessing Ethereum's Operational Resilience.

A Framework For Institutions Evaluating Public Blockchains

www.nethermind.io

CONTENTS

Table of Contents

01

Executive Summary

Ethereum is battle-tested and operationally resilient. Since its execution layer launched in 2015 and its consensus layer launched in 2020, the authors identified no full network halt or irrecoverable finality failure in the public incident record reviewed through August 4, 2026. It has also contained or recovered from the stress events assessed in this report — in some cases through protocol mechanisms alone, in others with client-team, infrastructure-provider or validator-operator intervention — including the September 2022 Merge, which transitioned the consensus mechanism without material service disruption. [01], [02]

As of July 2026, Ethereum's Staking Launchpad reported 885,351 validators and 39.45 million ETH staked. Network participation averaged 99.77% in Q1 2026. [71], [46] Notably, these results have been achieved through organically coordinated, decentralized operations rather than the directive of a single central operator, demonstrating outcomes consistent with the high-availability expectations typically applied to critical services.

Three mutually reinforcing defense layers help explain the track record.

1. The technical layer rests on client diversity. In this report, an Ethereum "client" is node software that implements the protocol — not a bank's customer or counterparty. Each node runs two independent clients: an execution-layer (EL) client (Geth, Nethermind, Besu, Erigon, Reth) that processes transactions, and a consensus-layer (CL) client (Lighthouse, Prysm, Teku, Nimbus, Lodestar, Grandine) that orders blocks and drives finality. Client diversity is the spread of validators across several independent implementations rather than one dominant one; it limits correlated-failure risk, because a bug confined to one client cannot impair validators running the others. The inactivity leak mechanism complements this by automatically preserving finality conditions under validator attrition without human intervention. [07]
2. The economic layer is correlated slashing, which penalizes coordinated misbehavior at a rate that scales with the fraction of validators involved, materially increasing the economic cost of coordinated validator misconduct, though not rendering every attack impossible. [10], [11], [12]
3. The social layer consists of the EIP process and All Core Developers (ACD) calls—the open forums through which client teams and researchers coordinate protocol upgrades—sustained across more than 100 biweekly calls and multiple successful hard forks. Section 6 explains this governance process in more detail. This provides structured protocol governance that is now complemented by the Ethereum Foundation's Trillion Dollar Security (1TS) initiative, announced in May 2025 and expanded through public reporting in 2025–2026. [23], [24]

A further historical technical control was the Holešky testnet, launched in September 2023 as Ethereum's largest public testnet for large-scale staking-infrastructure and validator-operations testing. Holešky reached end-of-life after Fusaka testing in October 2025; Sepolia and Hoodi are the currently maintained public testnets. [31]

Institutional alignment is now relevant. As of July 2026, RWA.xyz reported approximately $37 billion in distributed tokenized real-world-asset value, excluding stablecoins. [60]

Ethereum exchange-traded products provide material regulated exposure: BlackRock's ETHA reported $5.19 billion in net assets and its staked ETHB reported $536 million, both as of 14 July 2026. [57], [58]

As this regulated financial angle grows, Ethereum and its ecosystem will be expected to provide clearer information about standards, stress events, disruptions, incident reporting practices, and structured testing so that institutional participants can evidence resilience in terms familiar to their risk committees.

RWA.io and Veritas Protocol report $14.6 million in RWA-specific losses in H1 2025, versus $6.1 million in 2024; their analysis attributes the 2025 incidents to on-chain operational failures. [70] In discussing these incidents, attribution of where and how the losses occurred matters: application-layer vulnerabilities or operational failures in individual smart contract protocols (DeFi protocols) may be reported as "onchain" events, but they should not be assumed to be failures in Ethereum's base-layer consensus mechanism. The more accurate interpretation is that these losses are primarily associated with applications and operational controls and limitations, rather than vulnerabilities in Ethereum's consensus layer. [60]

Accordingly, differentiating smart contracts' weaknesses from the underlying blockchain's flaws is important to guide focus, solutions and resilience in institutional-friendly terms, to facilitate informed adoption, shared understanding, and constructive engagement as participation and volume scale. The next sections examine the remaining factors institutions should monitor.

First, consensus-layer client concentration warrants monitoring. Client Diversity's Miga Labs view, accessed on 23 July 2026, estimated Lighthouse at approximately 50.6% of consensus-client share; estimates vary by methodology. [49] This is above the commonly referenced one-third validator-weight threshold at which a correlated consensus-client failure can delay finality. It should therefore be treated as an active concentration risk rather than threshold proximity. Institutions should monitor methodology-consistent trends, maintain robust client release and regression controls, and diversify their own validator fleets.

Second, Ethereum does not yet operate a formalized resilience-testing program that is, for example, aligned to the EU's Digital Operational Resilience Act (DORA), although it embeds best practices from its expert communities; regulated institutions may draw on this infrastructure within their general DORA testing programmes (Articles 24–25), although threat-led penetration testing under Article 26 must run on live production systems and cannot be performed on testnets. Current assurances occur organically through testnet exercises and production learnings. [48], [51], [23], [52], [53], [54] On one hand, this reflects Ethereum's organic growth in the blockchain space, its battle-hardened resilience today and the intention of the community to preserve longevity and distribute opportunity. On the other hand, new resilience simulation studies can further deepen its resilience profile and facilitate seamless adoption by more of the regulated-industry participants.

Third, Ethereum's governance and incident-handling processes are largely community-driven. To facilitate growing institutional adoption, these can be complemented by clearer documentation of decision rights, escalation pathways, and incident-communication practices in forms familiar to risk frameworks. The Ethereum Foundation's Trillion Dollar Security (1TS) initiative has explicitly recognized these areas and is progressing work to strengthen them. [23], [24]

At this evolutionary juncture, the primary need is not further proof that Ethereum functions. It is clearer documentation, stronger application-development security practices, and assurance artifacts that translate Ethereum's resilience record into formats usable by institutional financial services teams, while avoiding disclosures that create new attack surfaces.

This implies two complementary tracks: one controlled by regulated institutions and one for the Ethereum community to consider voluntarily.

The first track highlights existing financial industry-grade controls that institutional operators — asset managers, custodians, staking providers and others — should be aware of and/or can adopt within their existing risk frameworks today.

This track would include client-diversification indicators across both execution and consensus layers, monitoring data requirements, institutional incident-response playbooks, and awareness of governance participation protocols. These controls also address the technology and governance risks highlighted by regulators such as the Monetary Authority of Singapore (MAS) in its review of prudential treatment for cryptoasset exposures on permissionless blockchains. [68] While the Basel Committee's SCO60 standard, effective from 1 January 2026, applies conservative Group 2 treatment to exposures using permissionless blockchains where the Group 1 classification conditions are not met, the standard is directly relevant to bank balance-sheet exposure.

The Basel Committee has previously expressed substantial concern about whether the risks associated with permissionless blockchains can be sufficiently mitigated. Under current SCO60, banks must assess each exposure against the Group 1 classification conditions on an ongoing basis; assets failing those conditions receive Group 2 treatment [75]. MAS's consultation (a paper proposing approaches, not a final standard) explores a more principle-based path for assessing whether permissionless-network risks can be sufficiently mitigated.

The second track is a voluntary, structured resilience formalization agenda for the Ethereum ecosystem that could build on and complement the 1TS initiative. This agenda would expand documented resilience testing, agreed approaches for incident disclosures, and governance transparency sufficient for regulatory consumption. [23], [24]

These steps build on Ethereum's existing strengths while improving alignment with institutional assurance expectations in financial services. They are intended to be practical and well defined, recognising both Ethereum's single global operating environment and the varied regulatory and supervisory expectations that apply across jurisdictions.

02

An Operational Resilience Framework for Ethereum

For Ethereum to be assessed with confidence by institutional participants and regulators, it needs to be evaluated against similar or equivalent rubrics that stakeholders apply to critical financial infrastructure. This section establishes a proposed framework drawing principally from the EU's Digital Operational Resilience Act (DORA), the FCA/PRA Operational Resilience framework and NIST CSF 2.0 [76], [77], with the Markets in Crypto-Assets Regulation (MiCA), the enacted GENIUS Act and the proposed CLARITY market-structure framework included as relevant digital-asset market context. [51], [52], [53], [54] It then maps Ethereum's architecture to each dimension.

Critically, this framework does not demand structural "sameness" with centralized systems. Rather, it asks whether the core outcomes that resilience regulation is designed to protect continuity of service, fault containment, proportionate security, governance integrity, and incident transparency are demonstrably achievable. Ethereum's case is that such outcomes are available, through mechanisms whose architecture is different from those of critical conventional financial market infrastructure and therefore presenting different strengths, limitations and assurance characteristics.

Framework Purpose and Scope

The framework would serve at least three audiences. First, for institutional risk committees, it provides a structure that is familiar and can be aligned with existing enterprise risk taxonomies. Second, for regulated institutions assessing how they can engage with Ethereum while operating under applicable operational-resilience, prudential and digital-asset regimes, it identifies where Ethereum's properties may support an institution's implementation of relevant requirements and where additional entity-level controls are needed. Third, for the Ethereum ecosystem, it defines the formalization agenda needed to close the gap between operational performance and the documentation that regulated industries require.

DORA, MiCA and the FCA/PRA operational-resilience rules apply to regulated entities and their services, not to Ethereum as a protocol. Ethereum characteristics discussed in this report may inform an entity's risk assessment or provide evidence relevant to particular control objectives. They do not, individually or collectively, establish regulatory compliance, which depends on the entity's governance, systems, contracts, testing, recovery arrangements, reporting obligations and particular use of Ethereum.

The proposed framework organises resilience across eight dimensions based on Ethereum as a public blockchain, although the same structure may be relevant to other public blockchains.

Dimension	Core Institutional Expectation
1. Operational Continuity & Availability	Institution-defined impact tolerances for each important business service, with supporting RTOs/RPOs; demonstrated ability to remain within the declared impact tolerance
2. Automated Fault Isolation & Self-Recovery	No undisclosed single points of failure; automated recovery with empirical validation
3. Concentration & Dependency Risk	Documented thresholds; concentration monitored and disclosed
4. Economic Security & Attack Deterrence	Proportionate economic deterrence; adversarial scenarios analyzed
5. Governance Integrity & Change Management	Auditable decision rights; formal change management; conflict of interest controls
6. Monitoring, Detection & Incident Communication	Real-time monitoring; defined notification timelines; standardised post-mortems
7. Structured Resilience Testing & Assurance	Repeatable testing calendar; adversarial scenario coverage; third-party validation
8. Transparency, Auditability & Governance Documentation	Accessible governance trail; documentation in institutional-compatible formats

The sections below apply this framework to Ethereum's empirical record.

Section 3 maps Ethereum's self-healing mechanisms to Dimensions 1–4 through the four documented stress events. Section 4 assesses the Resilience Architecture (client diversity, DVT, testnet strategy, and emerging certifications), including the economic-security controls relevant to Dimensions 2 and 4, against all eight dimensions. Section 5 examines the resilience testing gap (Dimension 7). Sections 6 through 9 address governance (Dimension 5), community splits (Dimensions 3 and 7), monitoring infrastructure (Dimension 6), and the institutional due diligence playbook (all dimensions).

03

Post-Merge Operational Record: Stress Events, Self-Healing, and Framework Implications

This report assesses four significant post-Merge mainnet stress events since September 2022. Ethereum's protocol-level finality protections operated without permanent finality loss, but full restoration of participation in the December 2025 event involved client-team guidance, runtime configuration changes, and operator action. The events assessed were operational in origin—software bugs and misconfigurations—rather than adversarial attacks on the protocol.

Examined through the aforementioned framework, each event constitutes an empirical test of specific dimensions. The pattern across all four events is that Availability, Fault Isolation, and Economic Security were validated under real conditions; whereas Concentration, Monitoring, Testing and Transparency each reveal areas that would benefit from further formalization.

Case 1: The Merge (September 15, 2022)

What happened: The transition from proof-of-work to proof-of-stake completed without material service disruption. The Merge completed at terminal proof-of-work block 15,537,393 (first proof-of-stake block 15,537,394) during Beacon Chain epoch 146,875 [01, 02], following more than two years of preparation: 100-plus biweekly All Core Devs calls, multiple merged testnets, and shadow forks [01].

The Merge is the most demanding operational continuity test Ethereum has undergone: a complete replacement of the core consensus mechanism without interruption to service. In conventional financial market infrastructure terms, this is analogous to replacing a central securities depository's settlement engine while markets remain open.

The upgrade path – comprising 100+ ACD calls, public EIP process, multiple testnet activations, and shadow forks, constitutes a documented, auditable change management process. Each decision point is publicly recorded on GitHub (ethereum/pm), providing a documented ICT governance and audit trail. The absence of a formal voting mechanism is partially offset by the completeness of the decision audit trail.

The pre-Merge testing program —multiple testnets, shadow forks, and deliberate stress scenarios — demonstrated structured pre-deployment validation. However, the testing was designed to validate a specific transition, not to constitute a repeatable adversarial resilience program. The gap lies not in the quality of testing, but in its continuity. We define 'rigour' as the depth and adversarial realism of testing: actively injecting faults, network partitions, and failure conditions into production-like environments. Ethereum demonstrates this rigour ahead of major upgrades. However, a continuous, scheduled, independent resilience and chaos-testing function that operates regardless of pending upgrades is currently absent at the ecosystem level. This is the type of ongoing testing

program that operational-resilience regimes such as DORA and periodic threat-led penetration testing expect from regulated institutions.

The Merge was successful and no recovery mechanism was required. Its relevance to the resilience framework is as a change-management benchmark: the highest-stakes upgrade in Ethereum's history was executed through a documented, testnet-validated process while the chain continued to run "on production" with full continuity of service. That is to say, Ethereum did not shut down for the upgrade but continued running while the upgrade happened. This result is a reference and baseline against which institutional upgrade risk assessments should be calibrated.

Case 2: May 2023 Beacon Chain Finality Delays

What happened: On May 11–12, 2023, two Beacon Chain finality delays occurred, lasting four and nine epochs respectively and triggering Ethereum mainnet's first inactivity leak. The Prysm post-mortem attributes approximately 47 missed blocks to the first incident and approximately 149 to the second—about 196 attributable missed blocks in total. [04]

The incidents were triggered when some consensus clients processed valid attestations referring to an old target checkpoint inefficiently. Prysm's state-regeneration and caching path caused resource exhaustion, while Teku was also affected. Client diversity limited the impact because unaffected clients continued producing blocks. The inactivity leak activated during the longer incident and imposed approximately 28 ETH in penalties, but finality returned when the affected clients recovered; the incident did not last long enough for the inactivity leak to materially reduce inactive validators' effective balances or restore finality through stake reweighting. [03, 04, 05, 06]. Protocol finality should not be conflated with legal settlement finality. In the EU, legal settlement finality is defined through the Settlement Finality Directive and the designation of qualifying systems; protocol finality is relevant evidence but is neither necessary nor sufficient to establish that legal status. The legal treatment also depends on the relevant system arrangements, instrument documentation and governing law. [74]

While finality was delayed, importantly, transactions and their eventual finality were not lost and the protocol continued producing blocks throughout the event.

When evaluating the resilience of Ethereum through this incident, the relevant question is whether the incident remained within declared impact tolerances. Currently, no formal tolerances are published for Ethereum at the ecosystem level. However, the empirical outcome, i.e. that the delay was bounded at under one hour and that there was no irrecoverable state, is consistent with what most institutional continuity frameworks would classify as a significant but recoverable incident.

No governance vote or emergency protocol patch was required. Client and operator activity still formed part of incident diagnosis and remediation, while the protocol's inactivity-leak mechanism operated automatically once its activation conditions were met. Recovery time is scenario-dependent: for a hypothetical case with 50% of stake offline, restoration is expected on the order of approximately two to three weeks rather than within hours. The May 2023 event empirically validated the mechanism under a materially less severe condition.

By analogy with business-continuity concepts used in ISO 22301, the mechanism provides a defined and empirically observed automated recovery path. ISO 22301 applies to an organisation's business continuity management system; this comparison does not imply that Ethereum is ISO 22301-compliant or certified. For institutional risk frameworks, this mechanism can be documented as a verified automated failover procedure [66].

The detailed post-mortem was published by the Prysm team (Offchain Labs), with fixes and release notes published by other client teams including Teku, demonstrating transparency. These materials were published at the discretion of individual teams rather than through a standardized ecosystem-wide cadence. [04], [05] This review identified no standardized ecosystem-wide incident-notification protocol. Regulated financial institutions must therefore maintain their own detection and escalation triggers, including channels with their Web3 collaborators and partners, rather than relying on ecosystem-level notification.

Case 3: December 2025 Fusaka/Prysm Incident

What happened: On December 4, 2025, a Prysm client bug introduced during a refactor surfaced immediately after the Fusaka upgrade, producing a stale-attestation failure mode similar to the May 2023 incident. The refactor recreated Capella-era conditions, triggering expensive historical state replays under high validator load. [17], [18], [32], [61]. The bug had been present in testnet code for approximately one month without triggering because the failure mode requires a large validator set with many validators out of sync. [17], [18]

Metric	Value
Affected range	Epochs 411,439–411,480 (42 epochs)
Missed blocks	248 out of 1,344 slots (18.5% missed slot rate)
Participation rate (trough)	75%

Metric	Value
Validator losses	~382 ETH (~$1M+) in missed attestation rewards
Finality status	Never lost

Finality was maintained throughout, despite the missed-slot rate reaching 18.5%. The affected 1,344-slot range—equivalent to 42 epochs, or approximately 4.48 hours—exceeded the May 2023 event in length but not in severity. Some summaries describe 41 missed epochs, while the inclusive affected range spans 42 epochs; this report uses 42 epochs for the range and 248 for the missed-block count. Given the continuity, the service remained operational through a significant but manageable degradation.

Risk management and blast radius containment were again robustly held through the client diversity mechanism. This time, the inactivity leak was not activated because finality was maintained. Prysm represented less than one-third of validator weight, so impairment of Prysm alone was insufficient to prevent the two-thirds participation required for finality. This highlights a two-stage defense layer here, with the automatic containment a validated system-level protection and the client diversity as another safeguard.

While the protocol contained the impacts, the incident nevertheless highlights the value of stronger regression controls across client implementations. The margin of safety is supported by maintaining client shares below commonly referenced concentration thresholds, a condition examined in Section 4, or a more rigorous higher standard on clients. This incident is instructive precisely because Prysm was not the largest consensus client. At an estimated 17–22% of validators, its impairment contributed to participation falling to approximately 75%, leaving roughly an eight-percentage-point margin above the two-thirds participation required for finality. A comparable failure affecting more than one-third of validator weight could prevent timely finality. The consequences at or above two-thirds would be more severe and would depend on the failure mode.

The recurrence of the identical bug class, the same Prysm PR 15965 pattern, 30 months after it was first identified is evidence that the current decentralized client development model does not yet fully operate with the regression-detection controls expected of critical system components under frameworks such as DORA, ISO 27001, and SOC 2. An organisation whose relevant systems fall within the scope of an ISO 27001 ISMS or a SOC 2 examination would ordinarily evaluate such an incident through its documented

incident-management, change-management and corrective-action controls. Urgent hotfixes can be deployed, but the workflow would typically include documentation, authorisation and testing appropriate to the organisation's documented controls. Neither ISO 27001 nor SOC 2 prescribe a specific test or implementation plan but the expectation is that corrective actions are evaluated and validated through the organisation's own control framework. The absence of equivalent controls across decentralized client teams is a gap at the ecosystem level. Institutional operators should factor this into their own change-management procedures and include a review of regression tests for previously identified bug classes in dominant client implementations during each Ethereum upgrade cycle.

Fusaka Devnet-3 had included the bug for approximately one month without triggering it. The failure mode depended on mainnet-scale validator numbers, synchronisation conditions, economic dynamics, and adversarial conditions that testnets cannot fully replicate. This reflects a structural limitation of current testing infrastructure, although the bug itself was a low-probability edge case. The lesson is not that every edge case can be tested in advance, even in regulated industry. It is that high-impact, low-probability scenarios should be explicitly considered in future testing, and that Ethereum's embedded defenses should be assessed for their ability to minimise impact and limit blast radius when recovery is required.

The specific mechanism of multi-client architecture in Ethereum, where minority clients continue producing blocks when the dominant client is impaired, is an architectural property rather than a procedural response, and one that regulators can evaluate as a structural control. The institutional-level implication is that validator fleet composition (CL and EL client selection) is itself a risk-management function.

Case 4: SSV Network Slashing (September 10, 2025)

What happened: Two separate slashing incidents occurred approximately 90 minutes apart. The first affected a single validator associated with a cluster that had previously migrated from Allnodes. The second affected a separate 39-validator cluster operated by Ankr, where a parallel validator instance was run during internal maintenance. SSV's founder confirmed that the protocol itself was not compromised. [13], [19] For context, the Beacon Chain launched on 1 December 2020. Fewer than 500 validators had reportedly been slashed cumulatively before the September 2025 incidents, which added 40 validators across two separate events. Because cumulative slashings, the active validator set and the ever-activated validator population use different denominators, this report does not present a single cumulative percentage without a dated, like-for-like dataset.

The slashing mechanism operated exactly as designed. Penalties were contained to the operators responsible for the duplicate key deployment, with zero impact on validators

not involved in the error. Additionally, the incident produced no network-level disruption. The 39-validator cluster represented less than 0.005% of the active set, depending on the dated active-validator denominator used. Fault isolation at the protocol level was complete and the broader network was unaffected. Protocol integrity was preserved, but remediation of the operator-level failures required investigation and operator action.

No network-level concentration risk was implied given that 39 validators are operationally immaterial at network scale. It does, however, directly implicate operational concentration risk at the staking provider level.

For institutional staking arrangements particularly post-Pectra, where consolidated validators carry up to 64x more ETH at risk, operator-level key management controls are an important concern. In an organisation whose relevant systems fall within the scope of a SOC 2 examination or ISO 27001 ISMS, duplicate key deployment during a maintenance window would ordinarily warrant assessment as a potential change-management control failure and, depending on the applicable control design and resulting findings, may require root-cause analysis and corrective action. The decentralized staking model does not apply a common change-management standard across operators. NORS certification—currently listed for Pier Two, Figment and Blockdaemon—addresses this gap at the operator level; the institutional implication is that staking provider selection should incorporate assessment of change-management maturity, not only technical performance metrics. [72] Separately, on 17 March 2026 the SEC and CFTC issued a joint interpretation identifying ether as a digital commodity and concluding that the Protocol Staking Activities described in the release, when conducted under the specified circumstances, do not involve the offer and sale of a security. The conclusion is fact-specific and should not be read as determining the treatment of every staking product or arrangement. [79]

SSV Network published an incident report confirming protocol integrity and identifying the operational root cause. For institutional investors in Ethereum staking products, this event should be incorporated into incident response playbooks as a reference case for the distinction between operator-level failures and protocol-level vulnerabilities.

The slashing mechanism is the most directly applicable economic defense addressing a risk also recognised by regulatory frameworks: hostile "takeover" attempts of the chain. It evidences proportionate security controls by design: the penalty scale makes large-scale coordinated attacks economically prohibitive while remaining proportionate for isolated operational errors. Institutions can document this mechanism as a validated economic deterrence control. Post-Pectra, the same mechanism requires updated risk documentation to reflect the changed effective balance parameters under EIP-7251. [14], [15], [16]

Summary: Framework Assessment Across All Four Events

Dimension	The Merge (Sep 2022)	May 2023 Finality	Dec 2025 Fusaka	SSV Slashing (Sep 2025)
D1 Continuity	✓ Met	✓ Met	✓ Met	✓ Met
D2 Fault Isolation	✓ N/A	✓ Validated	✓ Validated	✓ Met
D3 Concentration	– Monitor	⚠ Threshold proximity	⚠ Elevated concern	⚠ Operator-level
D4 Economic Security	– N/A	– N/A	– N/A	✓ Validated
D5 Governance	✓ Met	– Partial	⚠ Gap	⚠ Operator gap
D6 Monitoring	– Partial	⚠ Gap	⚠ Gap	⚠ Partial
D7 Testing	✓ Met (upgrade-specific)	⚠ Scale gap	⚠ Scale gap confirmed	– N/A
D8 Transparency	✓ Met	⚠ Partial	⚠ Partial	⚠ Partial

04

Resilience Architecture: Framework Assessment of Ethereum's Structural Controls

Ethereum's resilience architecture comprises four structural control categories: multi-client diversity, testnet-based pre-production validation, Distributed Validator Technology, and emerging institutional certification standards, each addressing distinct dimensions of the operational resilience framework. This section assesses each control against the relevant framework dimensions, identifies current gaps, and specifies the monitoring and due diligence requirements that follow.

The Central Tension

Two observations define the current state. First, proactive controls — testnet stress-testing, DVT adoption, and emerging certification frameworks — are advancing. Second, the most important consensus-layer concentration risk (Dimension 3) has at times moved in the opposite direction. This divergence — improving controls alongside rising concentration risk — is the central tension in Ethereum's current resilience profile and the lens through which all four control categories should be assessed.

Control 1: Multi-Client Architecture

Ethereum's infrastructure operates across two independent software stacks: the consensus layer (CL), where Lighthouse, Prysm, Teku, Nimbus, Lodestar, and Grandine each implement the PoS protocol independently; and the execution layer (EL), where Geth, Nethermind, Besu, Reth, and Erigon each process transactions and execute smart contracts. These are distinct codebases with separate failure modes and independent release cycles.

The architecture's independence and functional separation are detailed in the official consensus specifications and academic research on availability-finality trade-offs. [08], [65]

Framework Dimension 2 Fault Isolation: The multi-client architecture is the primary structural mechanism for Dimension 2. As demonstrated in May 2023 and December 2025, when a consensus client suffers a bug, validators running unaffected clients may continue operating and limit the correlated impact. This provides empirical evidence of fault isolation under the conditions assessed; it does not establish that recovery would be automatic under every client-share or failure scenario. The architecture is consistent with the protection, prevention and fault-tolerance objectives found in DORA-style ICT frameworks, including the redundancy and resilience requirements in DORA Articles 7 and 12. Its effectiveness depends on validator weight remaining sufficiently distributed across independent implementations. [09]

Framework Dimension 3 Concentration Risk: Client diversity is a strength when validator weight is distributed across independent implementations and a vulnerability when one implementation becomes too dominant. For consensus clients, one-third of validator weight is a practical prudential marker: a correlated failure affecting more than one-third can prevent finality until the affected validators recover or the inactivity leak sufficiently reweights participation. This is not a universal safe-or-unsafe boundary, and recovery time depends on the failure mode and remaining participation. Execution-client concentration must be assessed separately because its measurement methods, validator exposure and failure consequences differ; the consensus-layer one-third threshold should not be applied mechanically to execution-client estimates.

Dominant Client	Lighthouse	Prysm	Geth	Nethermind
Layer	Consensus	Consensus	Execution	Execution
Function	PoS protocol; attestations and block proposals	—	Transaction processing; smart contract execution	—
Estimated share (accessed July 2026)	~50.6% (Miga Labs view)	~22.0% (same view)	~40–43% (varies by methodology)	~38–43% (varies by methodology)
Reference threshold	<33%	<33%	<33%	<33%
Status	Above reference threshold; active concentration risk	Below reference threshold	Exceeded	Exceeded

Client-share estimates are methodology-dependent, particularly on the execution layer. The table should therefore be treated as a dated monitoring snapshot rather than a definitive measurement.

A consensus-client failure affecting more than one-third of validator weight can prevent finality. At or above two-thirds, correlated faults may create more severe safety and chain-consistency risks, depending on the failure mode. The May 2023 and December 2025 cases provide evidence of containment below those conditions; they do not demonstrate recovery from a supermajority-client failure. Execution-client concentration creates different risks, including divergent execution results, missed validator duties and degraded transaction processing, and should be assessed using validator exposure and

implementation-specific failure analysis. Both layers represent material Dimension 3 risks requiring explicit institutional monitoring and disclosure. [49]

CL and EL concentration must be assessed as two distinct exposures with separate mitigation requirements. A validator fleet running minority CL clients but Geth for execution has partially addressed the risk; a dual-layer client audit with independent diversity targets is the requisite baseline. Institutional operators should define their own internal thresholds (e.g., maximum 25% of their own validator fleet on any single client) even where the ecosystem-level threshold is exceeded.

What institutions can do: Monitor client concentration using methodology-consistent metrics and conduct monthly reviews. While any consensus client remains above one-third of validator weight, maintain an elevated-risk status, establish institution-level diversification limits and escalate any further sustained increase.

Control 2: Testnet Architecture

Ethereum's testnet architecture functions as a staged pre-production validation pipeline, where protocol upgrades are exercised at scale and under adverse conditions before any mainnet activation. The currently maintained public testnets are Sepolia and Hoodi, supplemented by purpose-built devnets for upgrade-specific testing. The now-deprecated Holešky testnet was historically used for large-scale validator and staking-infrastructure testing; Hoodi subsequently validated the Pectra upgrade path after problems on Holešky and Sepolia.

Framework Dimension 7 Testing and Assurance: Testnets constitute Ethereum's primary structured resilience testing infrastructure. They may contribute evidence to an institution's protocol-compatibility, upgrade and scenario testing, but they do not test the institution's complete service architecture and therefore do not, by themselves, satisfy DORA's entity-specific ICT testing requirements. The Pectra upgrade path i.e., Holešky failure (execution-client deposit-contract misconfiguration resulting in chain split), Sepolia failure (testnet-only deposit-contract misconfiguration), Hoodi success, then mainnet activation, demonstrates a genuine iterative testing discipline: the community did not proceed to mainnet before demonstrable readiness, building a third testnet when the first two failed [31, 32]. The developer-reported Fusaka Devnet-3 non-finality drill (deliberately triggered an extended non-finality period — the devnet stabilized after six days — to validate recovery procedures) demonstrates the technical capability for structured scenario testing.

Structural limitation (Dimension 7 gap): Testnet assurance has a documented, material constraint. The failure modes that caused the May 2023 and December 2025 incidents were not triggered on testnets because they require a validator set of May 2023 mainnet

scale (~560K, versus ~885K by July 2026) with specific synchronisation conditions that testnets could not reliably replicate. This represents a structural gap between severe-but-plausible scenario testing expected by operational-resilience regimes and what current testnet infrastructure can consistently deliver. The specific scenario classes not currently covered are enumerated in Section 6.

For EU-regulated institutions designated by their competent authorities, DORA stipulates mandatory Threat-Led Penetration Testing on live-production systems supporting critical or important functions at least every three years. DORA does not provide protocol-specific TLPT arrangements. A designated institution must scope and conduct TLPT for its own critical or important functions under Articles 26–27 and Delegated Regulation (EU) 2025/1190 [81]. Use-case-specific Ethereum scenarios may form part of the institution's threat-intelligence and testing work but do not replace the prescribed TLPT process. The Fusaka Devnet-3 drill demonstrates that the technical capability and institutional will for structured exercises exist; the gap is a systematic framework converting one-off drills into repeatable, auditable resilience assurance.

What institutions can do: Work with the ecosystem to improve testnet-to-mainnet scale ratio; increase and track severity and breadth of test; monitor number of third-party certified staking operators (NORS equivalent).

Control 3: Distributed Validator Technology Dimensions 2 (Fault Isolation) and 4 (Economic Security)

DVT uses threshold cryptography to split validator signing duties across multiple independent nodes. [33] A configurable threshold (e.g., 3-of-5 nodes) must agree before any attestation or block proposal is signed, reducing single-node and duplicate-key failure risks when correctly configured and operated, while introducing threshold-configuration, coordination and key-share-management considerations. DVT-lite offers a simplified approach to Distributed Validator Technology. It preserves the core availability benefit by using a containerized setup with automated operational coordination across multiple machines, with distributed signing underneath. This implementation automatically handles machine coordination, thereby reducing the overhead associated with cryptographically splitting the key.

Framework Dimension 2 Fault Isolation: DVT directly addresses the single-node failure mode that produced the selected slashing incidents examined in [63] and [64] in Ethereum's recent history (each was caused by simultaneous key deployment on two active nodes, the exact risk DVT's threshold signature eliminates). As a structural mitigation for Dimension 2, it converts single points of failure in validator infrastructure into fault-tolerant multi-node clusters. The Ethereum Foundation's treasury staking (deployment began 24 February 2026; target reached 3 April 2026) of 70,000 ETH using

DVT-lite constitutes a meaningful institutional endorsement of the technology's operational readiness. [34]

Framework Dimension 4 Economic Security (Post-Pectra relevance): The Pectra upgrade (EIP-7251) increased the maximum effective balance from 32 ETH to 2,048 ETH. Under the correlation penalty structure, a consolidated 2,048 ETH validator faces 64 times more ETH at risk than a 32 ETH validator in a mass slashing event. DVT is the architectural mitigation for this tail exposure: by reducing the duplicate-key failure mode implicated in the selected slashing incidents examined in this report, it directly reduces the Dimension 4 risk that Pectra's balance consolidation amplifies.

In its Q4 2025 Validator and Node Operator Metrics report (published March 2026), Lido reported that DVT was used across all its staking modules by 22,233 validators representing 711,456 ETH, or 1.99% of total Ethereum stake, as of 1 January 2026. Separately, its Community Staking Module and Simple DVT Module collectively represented nearly 800,000 ETH, or 2.2% of total Ethereum stake; because DVT use is voluntary within the Community Staking Module, this combined figure is not a measure of pure DVT adoption. [33] This review identified no publicly documented ecosystem-scale DVT stress event. Although DVT operates under real production workloads, its performance during system-wide conditions involving high validator load, synchronization failures or widespread partial node outages has not been independently demonstrated. Network latency sensitivity and key-share management complexity persist as implementation risks, particularly for DVT-lite where key security relies on operational controls rather than cryptographic splitting.

Institutions need to treat DVT as a strongly recommended mitigation particularly post-Pectra for large consolidated validators rather than a proven control. Conduct pilot deployments at non-critical validator cohorts before full migration. Apply change-management discipline (Dimension 5) to DVT deployment and migration procedures, since the SSV Network incident demonstrates that maintenance and migration procedures can create slashing risk.

What institutions can do: Monitor DVT adoption rate and engage ecosystem players that deploy DVT for shared learnings (% of validator ETH secured via DVT); monitor post-Pectra consolidated validator exposure as consolidating more ETH into a single key naturally concentrates your maximum exposure.

Control 4: Emerging Institutional Certification Standards Dimensions 6 (Monitoring), 7 (Testing), and 8 (Transparency)

As of July 2026, the NORS (Node Operator Risk Standard) directory lists Pier Two (July 2025), Figment (January 2026) and Blockdaemon (May 2026) as certified entities.

Figment publicly describes its result as Full NORS Certification. NORS establishes documented standards for uptime, incident response, and operational controls, an additional provider-level assurance artefact that institutional risk committees may consider in third-party due diligence. Adoption remains early, and NORS is not yet an industry-wide standard. [67], [72]

Framework Dimension 6 Monitoring and Incident Response: NORS-certified operators provide a documented incident response framework aligned with institutional standards. For regulated entities selecting staking providers under DORA's third-party risk requirements, certification status constitutes a verifiable due diligence signal rather than a self-assessment. Its value depends on the certification's scope, assessment period, criteria and assessor independence; it does not establish DORA compliance and does not replace contractual provisions, audit rights, ongoing monitoring, concentration-risk assessment, incident obligations or exit planning. DORA's ICT third-party-risk regime presupposes a contractual arrangement with an identifiable service provider. Ethereum itself is a permissionless network and is not a contractual counterparty capable of accepting audit rights, service levels, termination provisions or incident-notification obligations. The relevant DORA dependencies are therefore contractable providers such as staking operators, RPC and node-service providers, custodians and other intermediaries. MiCA-authorised crypto-asset service providers are themselves included among DORA financial entities. Under MiCA Article 68 and Delegated Regulation (EU) 2025/299, authorised CASPs must additionally maintain entity-specific arrangements for the continuity and regularity of their crypto-asset services — including management-body ownership, realistic annual testing, documented results, recovery objectives and specific consideration of disruptions affecting permissionless distributed ledgers. Ethereum monitoring, testnets and ecosystem communications may support these activities but do not replace the CASP's own continuity, testing, governance and client-communication procedures. While the lack of ecosystem-level standardised incident reporting protocol is partially mitigated by operator-level certification, institutions should prioritize certified providers and require incident communication SLAs in service agreements.

Framework Dimension 7 Testing and Assurance: NORS certification evaluates operational controls including resilience testing procedures at the provider level. As certification adoption grows across the staking ecosystem, it will increasingly function as an additional provider-level assurance source addressing the Dimension 7 gap at the operator level, even in the absence of an ecosystem-level formal testing program.

Framework Dimension 8 Transparency and Auditability: Third-party certification provides an independent attestation layer that supplements Ethereum's native transparency mechanisms (the EIP and ACD governance trail). For institutional risk

committees accustomed to SOC 2 reports or ISO 27001 certificates, NORS certification offers a familiar assurance format.

However, three listed certifications do not yet constitute an industry-wide standard. Figment's certification establishes a benchmark and demonstrates that institutional-grade operational requirements can be formalized within the staking ecosystem; it does not provide assurance about uncertified providers. Institutions should maintain a certification registry of staking providers under assessment and require certification or equivalent documented controls as a selection criterion.

What institutions can do: Monitor the number of staking providers with active NORS (or equivalent) certification and require certification or equivalent documented controls as selection criterion, maintain a certification registry of staking providers, escalation if a material counterparty staking provider does not have active certification within 12 months.

Architecture Assessment Summary: Framework Status by Control

Control	Dimensions Addressed	Current Status	Primary Gap	Monitoring Priority
Multi-client architecture	D2 (Fault Isolation), D3 (Concentration)	D2 validated in the incidents assessed; Lighthouse exceeds the consensus-layer one-third reference threshold, while execution-layer concentration is elevated but not directly comparable	Consensus-client concentration above one-third; methodology-dependent execution-client estimates; incomplete institution-level visibility across both clients used by each validator	High (monthly)

Control	Dimensions Addressed	Current Status	Primary Gap	Monitoring Priority
Testnet architecture	D7 (Testing and Assurance)	Upgrade-specific testing is comparatively mature; continuous adversarial and mainnet-scale replication remains limited	No ecosystem-level continuous simulation program; regulated institutions remain responsible for their own applicable testing obligations	Medium (per-upgrade)
DVT	D2 (Fault Isolation), D4 (Economic Security post-Pectra)	Adoption growing; not yet stress-tested on mainnet	Production track record limited; latency and key-managemen t complexity	Medium (quarterly)
NORS certification	D6 (Monitoring), D7 (Testing), D8 (Transparency)	Three providers listed in the NORS certification directory: Pier Two, Figment and Blockdaemon; adoption remains early and NORS is not yet an industry-wide standard	Market-wide adoption; institutional counterparty selection criteria	Medium (annual registry)

05

The Resilience Testing Gap: From Organic Stress to Structured Simulation

Ethereum does not yet operate a formalized chaos-engineering or disaster-recovery simulation program comparable to Netflix's Chaos Monkey or the EU's DORA Threat-Led Penetration Testing (TLPT) requirements. Resilience testing occurs organically, through testnet failures, production incidents, and ad hoc developer exercises, rather than through structured, adversarially designed simulation. This is an area for further formalization (rather than an architectural weakness) and is relevant to how regulated institutions evidence resilience and assurance under resilience frameworks.

What Exists Today

Three mechanisms currently serve as Ethereum's de facto resilience testing infrastructure:

Mechanism	Description	Limitation
Testnet stress testing (historical Holešky; current Sepolia and Hoodi)	Deliberate failure injection before mainnet upgrades	Includes some adversarial scenarios, but not a continuous or independently governed resilience-testing programme
Fusaka Devnet-3 non-finality drills	Developers deliberately triggered non-finality lasting ~6 days to validate recovery procedures [61]	One-off exercise; no repeatable protocol or documented playbook
Academic chaos engineering (ChaosETH)	Fault injection on execution-layer clients revealed asymmetric resilience profiles under system-call errors [48]	Academic scope; not integrated into production readiness processes

The ChaosETH findings are instructive: identical fault injections produced different outcomes across execution-layer clients, with some crashing under theoretically recoverable errors. [48] A structured program would systematically surface and remediate this asymmetry. In the absence of such a program, assurance signals are more likely to emerge from production learnings and testnet exercises rather than from repeatable simulation

What a Structured Formalization Agenda Could Include

Referencing financial sector practices — DORA TLPT, the Bank of England's CBEST framework — a voluntary but structured resilience program would address five scenario classes not currently covered:

Scenario Class	Current Ethereum Coverage
Mempool congestion and fee spike simulations	Ad hoc only
Consensus load testing at mainnet validator scale	Partial (testnet scale only)
DDoS targeting validators, builders, and relayers	Partial (Hive tests cover validators)
Coordinated client failure drills (execution and consensus layers separately)	Partial (Devnet aimed to catch bugs)
Cross-client recovery playbooks	No ecosystem-wide playbook identified

The Decentralization Tension

Mandating resilience testing on Ethereum is structurally different from mandating it on a corporate IT system. No single entity owns the network; ecosystem-wide testing schedules are therefore typically voluntary. The Ethereum Foundation's 1TS initiative, whose February 2026 dashboard tracks security posture across six dimensions including monitoring and incident response, [23], [24] is the most credible vehicle for voluntary coordination; but coordinating across hundreds of independent client teams, staking operators, and infrastructure providers benefits from further structured tools and mechanisms. The realistic path is voluntary but formalized: a documented testing calendar, published recovery playbooks, and cross-client drill results shared transparently with the ecosystem.

06

Hard Fork Governance: Upgrade Cadence, Coordination, and Continuity Weak Points

Ethereum's hard fork governance operates through off-chain social consensus without formal voting, binding arbitration, or SLA-equivalent for mainnet deployment dates.

This is deliberate design, not oversight. For institutional participants accustomed to documented change-management procedures and accountable decision authorities, the model can require additional interpretation and monitoring.

How the Mechanism Works

Protocol changes follow a structured but informal path through four mechanisms:

- **EIP process:** formal written proposals submitted to a public repository at eips.ethereum.org, versioned and extensively auditable [25]
- **All Core Devs (ACD) calls:** biweekly video calls where client teams, researchers, and contributors reach rough consensus on which EIPs advance [26]
- **Rough consensus model:** no vote is taken; the ACD chair synthesises discussion into a working agreement, with dissent recorded in public notes [25]
- **Validator signaling:** operators can signal readiness or concern, but this is advisory, not binding [27]

The governance trail is extensively auditable: EIP revision histories, ACD call recordings, agendas, and notes are publicly archived on GitHub (ethereum/pm) and YouTube, with substantive technical debate on ETHMagicians and ethresear.ch. [25], [26], [62] Institutional due diligence teams can reconstruct the decision history for any protocol change without relying on third-party summaries.

Key-Person Concentration

Research by Fracassi, Khoja, and Schär (University of Texas at Austin, University of Texas at San Antonio, and University of Basel, 2024) found that 10 individuals are responsible for proposing 68% of all implemented Core EIPs, and an average of 10 people per client implementation account for 80% of all software changes. [28]

The structural mitigant is the multi-client architecture: no single contributor's departure can halt the network, and the public EIP record allows new contributors to reconstruct context. The concentration risk bears on upgrade velocity and institutional continuity planning, not on network operation itself.

Governance Credibility Events

Two events since 2024 served as tests of the model's self-correction mechanisms:

Event	Date	Issue	Response
EigenLayer conflict-of-interest episode	2024	Researchers Justin Drake and Dankrad Feist held a considerable amount in EIGEN tokens while advising on restaking integration	EF pledged in May 2024 to formalize a COI policy (internal policy in place by November 2024); Drake and Feist relinquished their EigenLayer roles (announced November 2024) [44],[45]
EF leadership restructuring	March 2025	Community criticism of slow execution and insufficient institutional outreach	Miyaguchi's transition to President announced late February 2025; Wang and Stańczak announced as co-Executive Directors on 1 March 2025 (effective 17 March); scale-L1/blobs/UX mandate articulated in the June 2025 "Announcing Protocol" post [44], [45]

Both episodes demonstrate that the ecosystem can identify governance issues and respond. The correction mechanism relies on social pressure and voluntary actions rather than procedural enforcement which is a difference that institutional risk committees need to recognise and account for in their own assessments and processes.

Upgrade Cadence: The Strawmap Roadmap

The Ethereum Foundation's February 2026 "Strawmap" roadmap outlines two near-term upgrades and a longer-horizon finality target: [40], [41]

Upgrade	Target	Consensus-Layer Headliner	Key Consideration
Glamsterdam	H2 2026	EIP-7732 (ePBS)	Builder "free option": estimated exercise probability of 0.82% of blocks on average and up to 6% on high-volatility days, under the paper's model and historical-data assumptions [73]
Hegotá	2027	EIP-7805 (FOCIL)	Protocol-level censorship resistance via validator inclusion lists [38], [39]
Lean Ethereum / Minimmit research target	Directional ~2029 horizon	One-round consensus research direction	Research targets describe finality on the order of seconds (reported targets as low as approximately 8 seconds), with shorter slot times explored progressively [40], [41]

Glamsterdam's ePBS proposal would enshrine proposer-builder separation at the protocol level. Research on the proposed design estimates that the free-option condition would be exercised in approximately 0.82% of historical blocks on average under an eight-second option window, rising to as much as 6% on high-volatility days; these are model- and data-dependent estimates, not protocol guarantees. Institutional staking operators should treat the effect as a scenario input ahead of activation rather than as a fixed slot-miss assumption. [38], [73]

Schedule slippage is a normal feature of the process; roadmap dates are directional targets, not contractual commitments. Institutions should build 30–90 day contingency buffers into operational planning tied to named fork activations. The Lean Ethereum / Minimmit research direction explores one-round consensus and shorter slots, with research targets describing finality on the order of seconds (reported targets as low as approximately 8 seconds) on a directional ~2029 horizon. If achieved, that would materially change operational settlement assumptions—such as collateral-release triggers and reconciliation with off-chain systems—for tokenized financial products

currently designed around Ethereum's present finality profile. It would not, by itself, change the legal definition of settlement finality. [40], [41]

The governance model's auditability is a genuine institutional asset: a substantial portion of the formal decision trail is publicly traceable, although not every discussion, influence or decision input is public. The absence of formal voting and binding timelines is the corresponding liability, requiring institutions to monitor ACD calls and EIP repositories as part of ongoing operational due diligence.

07

Community Splits and Tokenized Asset Risk: What Discord Means for Regulated Products

A contentious hard fork producing a chain split could duplicate RWA tokens without duplicating the underlying legal claims. Holders of a tokenized treasury bond would hold two technical token records on two chains that may correspond to only one enforceable claim against the issuer, producing ownership ambiguity. The legal effect would depend on the issuance terms, governing law, the legally authoritative register and the roles of the issuer, custodian, CSD or other infrastructure operator; a technical duplicate does not necessarily represent a second enforceable claim, and whether a forked token constitutes the recorded financial instrument requires fact-specific legal analysis; this analysis is reasoned inference from the underlying frameworks. [29], [30]

The DAO Fork: The Governance Lesson That Persists

The 2016 DAO fork established the foundational principle [82]. A majority supported a state rollback; a minority rejected it and continued the original chain as Ethereum Classic, which persists today. The lesson is not the technical mechanics but the demonstrated fact that network participants always retain the right to follow whichever fork they choose. [29], [30] As transition may not be uniform across all participants, institutional contingency planning should have criteria for their choice, the timing when they should choose and the possibility to reverse the choice at a later date.

Modern RWA Implications at July 2026 Scale

With RWA.xyz reporting approximately $37 billion in distributed tokenized real-world-asset value, excluding stablecoins, as of July 2026 (a cross-chain total, not Ethereum-only), [60] a chain split would create immediate legal and operational coordination requirements across three stakeholder groups:

Stakeholder	Immediate Problem	Regulatory Exposure
Token issuers	Should establish contractual fork procedures covering the authoritative ledger, suspension criteria, communications, reconciliation and resumption (prudent controls, not universal statutory requirements)	Canonical-chain and legal-claim analysis under MiFID II, the Prospectus Regulation, CSDR and, where relevant, the EU DLT Pilot Regime

Stakeholder	Immediate Problem	Regulatory Exposure
Custodians	Settlement ambiguity across both chains; reconciliation failure	Safeguarding, depositary, reconciliation and settlement obligations depend on the legally recognised asset and applicable financial-instrument regime
Regulators	Legal status of each forked record depends on the instrument terms, authoritative register and applicable law	Where the record continues to represent a financial instrument, MiCA's Article 2(4)(a) exclusion remains relevant; another technical record may represent a different crypto-asset or no independently enforceable right

An issuer without pre-agreed fork procedures may expose holders to prolonged uncertainty and settlement suspension on tokenized securities. This is a direct operational issue for regulated products that rests on the issuer's decision regarding those tokenized securities. [29], [30]

L1 Stress Cascades to the Tokenized Asset Stack

Chain splits are tail events, and narrower L1 stress events illustrate potential downstream effects.

The May 2023 finality delays illustrate how L1 stress can propagate into L2-dependent workflows. Polygon zkEVM's bridge ordinarily allowed claims on Ethereum within 30–60 minutes, barring anomalous network conditions; because the claim transaction settles on Ethereum, delayed L1 finality can delay the point at which a cross-layer transfer is treated as final. Fixed optimistic-rollup challenge windows are protocol parameters and were not automatically extended; the immediate effect is delayed L1-finality-dependent confirmation rather than a longer challenge period. [42], [43]

Probability, Mitigants, and the Residual Risk

The probability of a contentious chain split is very low. Ethereum's social consensus has strongly favored continuity since 2016; economic incentives overwhelmingly favor a single canonical chain, as liquidity, developer activity, and institutional capital concentrate on the dominant fork; and the growing weight of regulated institutional participants creates a powerful constituency for coordination over fracture.

The residual risk is not the probability of a split but an absence of pre-agreed contingency frameworks. Institutions holding or issuing tokenized assets on Ethereum should treat fork contingency planning as standard operational risk documentation, covering three components: pre-agreed canonical chain declaration procedures with token issuers, custodian protocols for settlement suspension and resumption, and legal opinions on forked token classification under applicable securities law.

08

Institutional Visibility: Monitoring, Incident Reporting, and the 1TS Initiative

Institutional-grade monitoring tools exist and perform at production scale, but incident reporting practices vary across teams. The Ethereum Foundation's Trillion Dollar Security (1TS) initiative, launched in May 2025 with public reporting and dashboard-style transparency developing through 2025–2026, is a significant systematic effort to address this gap — a meaningful start, with further work in progress. [23], [24]

Monitoring Infrastructure

Three platforms anchor institutional Ethereum monitoring today:

Tool	Capability	Current Evidence
Beaconcha.in	Validator surveillance: missed attestations, slashing alerts, sync committee duties, block proposals; webhook endpoints; enterprise dashboards [55]	Live validator dashboard and alerting capabilities; no fixed capacity figure used [55]
Hypernative	Real-time monitoring, risk detection, and automated response; ML-driven detection covering a self-reported 300+ risk types; validator performance tracking (slashings, missed rewards, attestations)	Hypernative reports that it was selected by the Ethereum Foundation to monitor protocol health and operational security; no independently verified vendor-scale metric is asserted here [69]
Forta Network	Real-time transaction screening: OFAC sanctions, threat detection, vendor-reported sub-10ms (p95) latency	Forta reports that more than 780 million transactions had been screened across supported networks by January 2026 [56]

Institutions can build operational dashboards meeting internal risk committee standards without waiting for ecosystem-level formalization.

The 1TS Initiative: Transparent Identification of Areas to Strengthen

The 1TS initiative tracks Ethereum's security posture across six dimensions: UX/wallets, smart contracts, infrastructure, consensus, monitoring/incident response, and governance. As of July 23, 2026, its public dashboard listed 94 controls across those six

dimensions; this is a dated snapshot rather than a fixed denominator. [23], [24] The first report identified six critical challenges:

Challenge Area	Specific Risk Identified
UX / Wallets	Blind signing exposure in hardware and software wallets
Smart Contracts	Upgrade mechanism risks in proxy contract patterns
Infrastructure	Centralisation of RPC endpoints, DNS, and cloud providers
Consensus	Edge cases in validator client behavior under stress
Monitoring / Incident Response	Inadequate detection and coordination during incidents
Governance / Social Layer	Staking centralisation and coordination failure risks

Source: 1TS initiative first report, 2025. [23, 24]

The infrastructure centralisation finding maps directly to third-party dependency risks that institutional risk committees flag in vendor assessments. The significance is not the list itself, but that the Ethereum Foundation is publicly tracking these gaps rather than papering over them — a governance signal that carries weight for institutional due diligence.

What Remains Missing

The 1TS dashboard is a tracking mechanism, not a resolution. Three structural process gaps remain:

- **No standardised incident reporting protocol:** Incident reporting is not yet standardised across the ecosystem: when a stress event occurs, communication flows through informal channels with no defined notification hierarchy or timeline.
- **No formal post-mortem publication cadence:** Post-mortem publication cadence is not yet standardised: incident analyses appear at the discretion of individual client teams rather than on a committed schedule

- **No SLA-equivalent for stress-event communication:** Stress-event communication does not follow an SLA-equivalent model: no defined maximum time-to-notification or minimum information standard exists today.

These improvements would materially help, but institutional participants still need to maintain their own incident-response procedures rather than relying on ecosystem-level coordination. [48], [23], [51]

The Walkaway Test: The Long-Term Resilience Benchmark

In January 2026, Vitalik Buterin articulated the long-term resilience benchmark: Ethereum must pass a "Walkaway Test," meaning the protocol should keep running safely and remain useful even if core developers paused major upgrades entirely. [59] The technical prerequisites — post-quantum cryptography, ZK-EVM validation of the execution layer, full account abstraction, and sustainable proof-of-stake economics — define the protocol's long-term self-sufficiency threshold.

This framing signals that EF leadership is designing toward a protocol that does not depend on continued centralized stewardship. Progress toward that threshold is expected to take multiple upgrade cycles. [40], [41]

09

Governance Due Diligence Playbook for Institutional Risk Committees

Institutional risk committees can conduct rigorous governance due diligence on Ethereum using entirely public records — but without a structured framework, most institutions either over-rely on third-party summaries and/or miss governance signals altogether. The five-pillar framework below converts Ethereum's public governance infrastructure into a repeatable assessment protocol.

The Five-Pillar Framework

Pillar	What to Assess	Primary Data Sources
1. Decision-making transparency	EIP lifecycle completeness, ACD call regularity, forum deliberation quality	eips.ethereum.org, github.com/ethereum/pm, ethresear.ch, ETHMagicians
2. Key-person and concentration risk	EIP authorship distribution, client team headcount, contributor turnover	EIP repository commit history, client GitHub repos
3. Conflict-of-interest controls	COI policy scope, disclosure completeness, enforcement record	EF blog, ACD notes, public disclosures
4. Upgrade risk management	Testnet failure rates, rollback capability, deployment timeline adherence	Devnet post-mortems, ACD call notes, client release logs
5. Stakeholder alignment	Validator concentration by operator, staking economics, community sentiment	Beaconcha.in, Rated.network, governance forums

Pillar 1 — Decision-Making Transparency.

Ethereum maintains an unusually extensive public governance and technical-decision trail, although not every discussion or decision input is necessarily public: EIPs are versioned text files with complete revision histories, all ACD call recordings and notes are archived on GitHub and YouTube, and ETHMagicians and ethresear.ch host the substantive technical debates that precede ACD decisions. [25], [26], [27], [62] There is no formal voting mechanism and no binding SLA for mainnet deployment dates; the audit question is therefore whether rough consensus is documented and traceable, not whether it is procedurally codified.

Pillar 2 — Key-Person and Concentration Risk.

Ten individuals account for 68% of all implemented Core EIPs, and approximately 10 contributors per client team account for 80% of software changes. [28] Flag any individual whose departure would remove more than 15% of active EIP authorship or client maintainership. Key-person risk at the authorship level does not translate directly into deployment risk — multi-client architecture means no single developer controls all implementations — but contributor attrition in a single client team can delay an upgrade cycle.

Pillar 3 — Conflict-of-Interest Controls.

Following the EF's May 2024 pledge — made after researchers Justin Drake and Dankrad Feist received a considerable amount in EIGEN tokens — an EF-wide internal conflict-of-interest policy was in place by November 2024, under which EF researchers are expected to disclose financial interests in projects they discuss in governance contexts. [44], [45] Committees should verify: (a) whether the policy covers all active protocol contributors or only EF employees; (b) whether disclosures are publicly logged; and (c) whether enforcement has been applied since adoption. The March 2025 leadership restructuring, installing co-Executive Directors Hsiao-Wei Wang and Tomasz Stańczak with an explicit execution mandate, is a second data point in the same corrective pattern. [44], [45] The pattern of institutional response matters more than any individual incident.

Pillar 4 — Upgrade Risk Management.

Assess each planned upgrade against three criteria: testnet coverage breadth, documented rollback capability, and explicit acknowledgment of known trade-offs in EIP documentation. The Pectra upgrade path — Holešky failure, Sepolia failure, Hoodi success, mainnet activation — is the reference case for how the ecosystem stress-tests before deployment. Budget for 30–90 days of schedule slippage on any named fork as a practical planning heuristic.

Pillar 5 — Stakeholder Alignment.

Coinbase validators represented 12.17% of total staked ETH, on average, in Q1 2026. Lido reported a 23% share of total staked ETH in February 2026; its governance-level concentration across operator selection, fee structures, and withdrawal credential control via Lido DAO remains material regardless of operational distribution across independent node operators. [46], [47]

Signal Register

Signal	Assessment Action
EIP authorship concentration increases sharply within one upgrade cycle	Investigate contributor attrition; request client team succession disclosures
Governance credibility event with no documented corrective action within 90 days	Escalate to risk committee; request EF written response
Testnet failure not followed by published root-cause analysis	Treat as upgrade risk management gap; delay mainnet exposure increase
Single operator or custodian approaches 33% of staked ETH	Reassess validator counterparty concentration in staking arrangements
Full EIP lifecycle documented with public debate records	Confirms decision-making transparency [25], [26], [62]
COI policy with logged disclosures and demonstrated enforcement	Confirms conflict-of-interest controls are operational [44], [45]
Multi-client architecture maintained across both execution and consensus layers	Structural check on centralisation
1TS dashboard publishes progress across all six dimensions and 94 controls listed as of July 23, 2026	Confirms proactive transparency trajectory

Implementation. Three data sources cover the majority of ongoing monitoring: the ethereum/pm GitHub repository (ACD call notes, updated biweekly), the 1TS public dashboard at trilliondollarsecurity.org, and on-chain validator distribution data via Beaconcha.in or Rated Network. Recommended cadence: a quarterly governance review covering pillars 1, 2, 3, and 5; and a per-upgrade risk assessment triggered by each mainnet hard fork announcement, covering pillar 4. Findings map directly into standard enterprise risk management categories — operational risk (governance concentration, key-person exposure), technology risk (upgrade cadence, testnet validation), and third-party risk (staking provider concentration) — without requiring a bespoke taxonomy

10

Conclusion

This paper has examined Ethereum's operational track record not to argue that it is risk-free, but to surface the mechanisms that have, in practice, contained or supported recovery from the four significant events assessed in this report. Those mechanisms are not always visible when applying traditional financial infrastructure frameworks, and that invisibility is itself a risk: misreading the architecture means misreading both its strengths and its genuine residual exposures.

The goal here is not to certify Ethereum as safe. It is to describe what is actually happening beneath the surface and to propose that resilience assessment should follow evidence rather than assumption.

Resilience Is Expressed Differently Here

Traditional financial market infrastructure achieves resilience through contractual SLAs, binding regulatory examination, centralized incident response, and legal liability for failures. The absence of these instruments in a decentralized network is often read as a deficiency. It is more accurate to read it as a different architecture.

Ethereum's resilience is expressed through cryptographic and economic mechanisms embedded in the protocol, through client diversity that limits blast radius, through penalty mechanisms that respond to failures automatically, and through a governance process that is slower to act than a corporate board while providing an unusually extensive public technical record — though lacking some formal accountability mechanisms present in regulated institutions.

Neither model is unconditionally superior. Centralized governance can act quickly and enforce accountability; it also creates single points of failure and concentration risk. Decentralized governance distributes that risk while introducing coordination challenges and key-person dependencies of a different kind. One relevant question for risk assessors is whether comparable resilience outcomes — continuity of service, incident transparency, governance accountability — are present in the architecture under review. This does not displace the formal governance, documentation, contractual or regulatory requirements applicable to regulated entities, and regulators may require both outcomes and prescribed legal or organisational forms.

The Position This Evidence Supports

Five evidence points support a positive assessment of Ethereum as core infrastructure:

- Continuous operation since Ethereum's 2015 launch, with no full halt of transaction processing identified in the operational record assessed in this report

- No irrecoverable finality failure across the post-Merge stress events assessed here; finality was delayed in May 2023, not permanently lost
- As of July 2026, 885,351 validators and 39.45 million ETH staked; Q1 2026 network participation averaged 99.77% [71], [46]
- Protocol defenses, including inactivity leak and slashing penalties, that operate automatically when their protocol conditions are met, as observed in the applicable events assessed
- Emerging institutional tooling: NORS-certified operators (currently Pier Two, Figment and Blockdaemon), Beaconcha.in enterprise monitoring, and Forta detection capabilities provide third-party assurance signals for risk committees [72]

One comparison requires qualification. Traditional financial market infrastructures operate under binding SLAs, mandatory regulatory examination, and legal liability for failures. Ethereum offers cryptographic and economic assurances rather than contractual ones: a different assurance model that is not directly comparable with contractual and regulated infrastructure.

Some Signals Should Be Monitored Continuously

Acknowledging Ethereum's resilience mechanisms does not require dismissing its open questions. Three warrant ongoing attention.

- **Consensus-layer client concentration.** The structural fault-isolation benefits of multi-client architecture diminish as any single implementation's validator weight increases. With Lighthouse currently estimated above the one-third prudential marker, this represents an active concentration risk rather than mere threshold proximity, particularly as no formalized ecosystem-level mechanism exists to enforce redistribution. Execution-layer dominance requires parallel monitoring using methodology-consistent metrics tailored to that layer's specific failure consequences.
- **Structured resilience testing.** Testnet exercises provide meaningful pre-production validation but do not yet constitute a repeatable, adversarially designed program.
- **Incident communication.** Post-mortem publication and stress-event notification remain informal and discretionary.

Caveat	Regulatory Relevance	Status
No formal resilience testing framework	No ecosystem-wide independent validation of recovery procedures; institution-specific testing remains necessary [51], [48]	Testnet drills provide supplementary evidence but are not substitutes for institution-specific testing or TLPT
Consensus-layer client concentration	ICT concentration risk; failure modes differ by layer	Multi-client architecture limits blast radius. Market share trend warrants monitoring
No SLA-equivalent for upgrades or incident communication	Complicates DORA incident reporting obligations and board escalation timelines	Institutions should define internal escalation triggers independently
EIP authorship and client development concentration	Key-person risk in small contributor cohorts	Public auditability and multi-client deployment prevent unilateral control
Governance operates through social consensus rather than formal accountability mechanisms	Governance trail is auditable; governance authority is not formally constituted	Documented self-correction events demonstrate working functional accountability
Relay-selection and censorship-resistance trends warrant ongoing monitoring; the applicable sanctions context has changed since the 2022 peak	OFAC-compliant relay usage rose from approximately 9% to 79% shortly after the Merge, but subsequently fell materially. OFAC also removed Tornado Cash from the sanctions list in March 2025, changing the legal context behind the original signal [80] [36], [37]	MEV-Boost is optional; institutional validators should document their relay-selection rationale as a risk-management and governance control

Ongoing Assessment, Not a One-Time Stamp of Approval

Resilience assessment of infrastructure that evolves through community-driven upgrades on a frequent cadence cannot be performed once at onboarding and filed away. The governance due diligence playbook in Section 9 and the monitoring dimensions in the Appendix are designed for exactly this reason: they convert Ethereum's public governance infrastructure into a repeatable assessment protocol that maps directly into standard enterprise risk management categories.

Institutions that treat Ethereum as a black box to be assessed once will miss the signals that matter. Institutions that monitor it as a live system, one that tracks client concentration, upgrade cadence, governance events, and validator distribution, will be better positioned both to manage their own exposure and to engage constructively with regulators who are still forming their understanding of what resilience looks like in this environment.

Ethereum's resilience mechanisms are real, empirically validated across four operational cases assessed since September 2022, and expressed through structural properties — client diversity, correlated slashing, inactivity leak, and governance auditability — that are frequently underweighted by parties applying frameworks designed for different architectures.

In regulatory terms, the position this evidence supports is deliberately bounded: Ethereum exhibits technical and governance characteristics relevant to several risks addressed by institutional operational-resilience frameworks. These characteristics may provide useful evidence within regulated institutions' own assessments and control programmes. They do not make Ethereum DORA-, MiCA-, FCA/PRA-, ISO- or SOC 2-compliant, and they do not establish that any institution or Ethereum-based product satisfies the applicable requirements.

The appropriate posture is to assess those mechanisms on their own terms: does operational continuity hold under stress? Is governance traceable? Are economic incentives aligned against catastrophic failure? The record documented in this paper answers each of those questions affirmatively, while being transparent about the conditions under which that record was built and the areas where further formalization would strengthen it.

Ethereum should be evaluated on the evidence it presents and the mechanisms it operates, not on its resemblance to infrastructure that preceded it. That evaluation, conducted rigorously and updated continuously, is what this paper intends to arm readers with.

11

Bibliography

Sources are organized by category and keyed to the source IDs used throughout the report.

Ethereum Foundation and Protocol Documentation

[01] Ethereum Foundation. "The Merge." ethereum.org. September 2022.

[02] Ethereum Foundation. "The Merge — Technical Summary." ethereum.org. September 15, 2022.

[07] Ethereum Foundation. "Beacon Chain Inactivity Leak." ethereum.org.

[08] Ethereum Foundation. "Ethereum Proof-of-Stake Consensus Specification." github.com/ethereum/consensus-specs.

[10] Ethereum Foundation. "Slashing Penalty Specification." consensus-specs.

[11] Ethereum Foundation. "Validator Penalties and Correlation Penalty." ethereum.org.

[12] Ethereum Foundation. "Slashing Mechanics." ethereum.org.

[14] Ethereum Foundation. "EIP-7251: Increase the MAX_EFFECTIVE_BALANCE." eips.ethereum.org. 2024.

[15] Ethereum Foundation. "Pectra — EIP-7251 Slashing Penalty Changes." eips.ethereum.org. May 2025.

[16] Ethereum Foundation. "Pectra Mainnet Activation." May 7, 2025.

[23] Ethereum Foundation. "Trillion Dollar Security Initiative." trilliondollarsecurity.org. Announced May 14, 2025; dashboard launched February 5, 2026.

[24] Svantes, Fredrik; Stark, Josh. "1TS Initiative: Security Challenges Report." Ethereum Foundation. 2025–2026.

[25] Ethereum Foundation. "Ethereum Improvement Proposals." eips.ethereum.org.

[26] Ethereum Foundation. "All Core Devs Call Archive." github.com/ethereum/pm.

[27] Ethereum Foundation. "Ethereum Governance Overview." ethereum.org.

[34] Ethereum Foundation. "DVT-Lite Staking — 70,000 ETH Deployment." February 2026.

[37] Ethereum Foundation. "Post-Merge Censorship Analysis." 2022.

[38] Ethereum Foundation. "EIP-7732: Enshrined Proposer-Builder Separation (ePBS)." eips.ethereum.org.

[39] Ethereum Foundation. "EIP-7805: Fork-Choice Enforced Inclusion Lists (FOCIL)." eips.ethereum.org.

[40] Ethereum Foundation. "Ethereum Strawmap Roadmap." February 2026.

[41] Chou, Brendan Kobayashi; Lewis-Pye, Andrew; O'Grady, Patrick (Commonware). "Minimmit: Fast Finality with Even Faster Blocks." arXiv:2508.10862. August 2025.

[43] Polygon Labs. "Announcing Polygon Bridge for Polygon zkEVM." April 26, 2023.

[44] Ethereum Foundation. "Conflict-of-Interest Policy." May 2024.

[45] Ethereum Foundation. "Leadership Restructuring Announcement." March 17, 2025.

[59] Buterin, Vitalik. "Ethereum itself must pass the walkaway test." X post, January 12, 2026. https://twitter.com/VitalikButerin/status/2010621884811845708

[62] ETHMagicians Forum. ethmagicians.org; Ethereum Research Forum. ethresear.ch.

[73] Mazorra, Bruno; Öz, Burak; Schlegel, Christoph; Wu, Fei. "The Free Option Problem of ePBS." arXiv:2509.24849. September 29, 2025.

Academic and Technical Research

[09] Buterin, Vitalik et al. "Parametrising Casper: The decentralization/Finality Time/Overhead Tradeoff." ethresear.ch.

[28] Fracassi, Cesare; Khoja, Moazzam; Schär, Fabian. "Decentralized Crypto Governance? Transparency and Concentration in Ethereum Decision-Making." SSRN 4691000, January 10, 2024. https://doi.org/10.2139/ssrn.4691000

[48] ChaosETH Research Team. "ChaosETH: Chaos Engineering for Ethereum Clients." 2023.

[65] Neu, Joachim; Tas, Ertem Nusret; Tse, David. "Ebb-and-Flow Protocols: A Resolution of the Availability-Finality Dilemma." IEEE S&P. 2021.

[66] Edgington, Ben. "The Inactivity Leak." Upgrading Ethereum.

Incident Reports and Post-Mortems

[03] Edgington, Ben. "What Happened During the Ethereum Finality Incident." beaconcha.in / Consensys. May 2023.

[04] Prysm Team. "May 2023 Finality Incident Post-Mortem." github.com/prysmaticlabs. May 2023.

[05] Teku (ConsenSys). "Teku 23.5.0 Release." github.com/Consensys/teku/releases. May 2023.

[06] Ethereum Cat Herders. "May 2023 Finality Delay Summary." May 2023.

[13] Migalabs / Rated Network. "Ethereum Slashing Statistics." migalabs.io. September 2025.

[17] Offchain Labs / Prysm Team. "Fusaka Upgrade Prysm Incident Report." December 2025.

[18] Prysm Team. "Fusaka Incident Root Cause Analysis — PR 15965." github.com/prysmaticlabs. December 2025.

[19] SSV Network. "September 2025 Mass Slashing Incident Report." September 2025.

[31] Ethereum Foundation. "Holešky Testnet Shutdown Announcement." September 1, 2025.

[32] Ethereum Foundation. "Hoodi Testnet Launch and Pectra Activation." March 2025.

[42] Offchain Labs. "Post-Mortem Report: Ethereum Mainnet Finality (05/11/2023)." May 18, 2023.

[61] Ethereum Core Developers. "Fusaka Devnet-3 Non-Finality Stress Test." 2025.

[63] Lido Finance / RockLogic. "April 2023 Slashing Incident Report." Lido DAO vote June 30, 2023.

[64] Lido Finance / Launchnodes. "October 2023 Slashing Incident Report." October 2023.

Regulatory Frameworks

[29] European Parliament and Council. "Directive 2014/65/EU on Markets in Financial Instruments (MiFID II)." 2014.

[30] European Parliament and Council. "Regulation (EU) 2022/858 on a pilot regime for market infrastructures based on distributed ledger technology." 2022.

[51] European Parliament and Council. "Digital Operational Resilience Act (DORA) — Regulation (EU) 2022/2554." Fully applicable January 17, 2025.

[52] European Parliament and Council. "Markets in Crypto-Assets Regulation (MiCA) — Regulation (EU) 2023/1114." ART/EMT provisions applied from June 30, 2024; most remaining provisions from December 30, 2024; Member State transitional arrangements for certain existing CASPs until no later than July 1, 2026.

[53] United States Congress. "GENIUS Act." Signed into law July 18, 2025.

[54] United States Congress. "Digital Asset Market CLARITY Act of 2025." Passed the House in July 2025; Senate process ongoing as of July 2026.

[68] Monetary Authority of Singapore. "Consultation Paper on the Prudential Treatment of Cryptoassets on Permissionless Blockchains". April 2026.

[74] European Parliament and Council. "Directive 98/26/EC on settlement finality in payment and securities settlement systems (Settlement Finality Directive)." 1998.

[75] Basel Committee on Banking Supervision. "SCO60: Cryptoasset exposures." Basel Framework. Effective January 1, 2026.

[76] National Institute of Standards and Technology. "The NIST Cybersecurity Framework (CSF) 2.0." February 2024.

[77] Financial Conduct Authority. "PS21/3: Building operational resilience." / Prudential Regulation Authority. "SS1/21: Operational resilience: Impact tolerances for important business services." March 2021.

[78] European Commission. "Commission Delegated Regulation (EU) 2024/1772 (incident classification); Commission Delegated Regulation (EU) 2025/301 (report content and time limits); Commission Implementing Regulation (EU) 2025/302 (reporting templates) — under DORA." 2024–2025.

[79] U.S. Securities and Exchange Commission and Commodity Futures Trading Commission. "Application of the Federal Securities Laws to Certain Types of Crypto Assets and Certain Transactions Involving Crypto Assets." Joint interpretation, Release No. 33-11412. March 17, 2026.

[80] U.S. Department of the Treasury, Office of Foreign Assets Control. "Tornado Cash Delisting from the SDN List." March 2025.

[81] European Commission. "Commission Delegated Regulation (EU) 2025/1190 — regulatory technical standards specifying the elements related to threat-led penetration testing under DORA." 2025.

[82] Ethereum Foundation (Buterin, V.). "Hard Fork Completed." blog.ethereum.org. July 20, 2016.

Institutional Tooling and Certifications

[33] Lido. "Lido Validator and Node Operator Metrics: Q4 2025." March 11, 2026.

[55] Beaconcha.in. "Beaconchain Dashboard." Accessed July 2026.

[56] Forta. "Financial Institutions Need Compliance Infrastructure. Forta Firewall Delivers It." January 27, 2026.

[67] Figment. "Setting a Higher Bar for Institutional Staking: Figment Achieves NORS Full Certification for Ethereum." February 4, 2026.

[69] Hypernative. "Hypernative Picked by Ethereum Foundation to Enhance Protocol Security." April 3, 2025.

[70] RWA.io and Veritas Protocol. "RWA Security Report 2025: An Analysis of Tokenized Asset Threats." October 2025.

[72] NORS. "NORS Certified Entities." Certification directory; accessed July 23, 2026.

Market Data, MEV Infrastructure, and Community Sources

[35] Flashbots. "MEV-Boost Relay Market Share Data." flashbots.net. 2025.

[36] mevwatch.info. "OFAC-Compliant Block Statistics." 2022–2025.

[46] Coinbase. "Ethereum Validator Performance Report Q1 2026." May 13, 2026.

[47] Lido. "Recap: Lido Tokenholder Update: February 2026." February 2026.

[49] Client Diversity. "Ethereum Client Diversity Dashboard." Daily dashboard; accessed July 23, 2026.

[57] BlackRock. "iShares Ethereum Trust ETF (ETHA) fund data." Accessed July 14, 2026.

[58] BlackRock. "iShares Staked Ethereum Trust ETF (ETHB) fund data." Accessed July 14, 2026.

[60] RWA.xyz. "Analytics on Tokenized Real-World Assets." Distributed tokenized real-world-asset value, excluding stablecoins; accessed August 2026.

[71] Ethereum Foundation. "Staking Launchpad." Live network statistics; accessed July 23, 2026.

12

Appendix: Continuous Monitoring. Key Systems and Metrics by Dimension

The monitoring triggers below are illustrative institution-set thresholds proposed by the authors. They are not Ethereum protocol thresholds, regulatory requirements or universal industry standards.

Given the eight-dimension framework established in Section 2, the tables below identify Ethereum system metrics that can indicate operational performance. Institutions should monitor relevant metrics continuously or at the stated cadence. These are operational signals intended to inform recurring governance reviews and, where applicable, regulatory reporting; they are not one-time assessments.

Dimension 1 Operational Continuity and Availability

Metric	Monitor For
Epoch finalization rate (% of epochs finalizing on schedule)	Any sustained deviation from >99.9%
Attestation participation rate (% of expected attestations included)	Drops below 94% across two consecutive epochs
Missed block rate (missed slots / total slots per epoch window)	Spikes above historical baseline (~0.5%)
Inactivity leak trigger events (count of mainnet activations)	Any activation; track duration and penalty depth
Validator uptime (% of active validators performing duties per epoch)	Drops below 98% at network level

Recommended cadence: Real-time alerting for finalization failures; weekly review of participation and uptime trends; quarterly summary for risk committee reporting.

Dimension 2 Automated Fault Isolation and Self-Recovery

Metric	Monitor For
Inactivity leak onset-to-recovery time (hours from trigger to finality restoration)	Benchmark: scenario-dependent recovery; approximately two to three weeks for a hypothetical 50% offline case
Time-to-containment per stress event	Increasing duration over successive events

Metric	Monitor For
Number of clients that remained live during a stress event (containment breadth)	Any incident where fewer than 2 minority clients remained fully operational
DVT adoption rate (% of validator ETH secured via DVT or DVT-lite)	Directional trend; benchmark against institutional commitment thresholds

Recommended cadence: Per-incident review for recovery metrics; quarterly trend analysis for DVT adoption.

Dimension 3 Concentration and Dependency Risk

Metric	Monitor For
Consensus-layer client share dominant client (%)	Lighthouse (or any successor dominant client) above 33%
Execution-layer client share dominant client (%)	Geth (or successor) above 33%
Staking operator concentration top operator / top 5 operators (% of staked ETH)	Any single operator above 15%; top 5 combined above 33%
Liquid staking protocol concentration top protocol (% of staked ETH)	Lido or successor above 33%
Cloud provider concentration (% of validators on AWS / GCP / Azure)	Any single cloud provider above 33%
RPC endpoint concentration (% of traffic through major providers: Infura, Alchemy)	Directional trend; no defined threshold yet, flag for monitoring

Recommended cadence: Monthly client concentration review; quarterly operator and cloud concentration assessment; immediate escalation while any consensus client exceeds one-third of validator weight; use separate institution-defined triggers for execution clients, operators and infrastructure providers.

Dimension 4 Economic Security and Attack Deterrence

Metric	Monitor For
Cumulative slashing rate (total slashed validators / total ever-active validators)	Any sustained increase relative to a clearly dated baseline calculated using the same denominator
Slashing correlation score (average % of stake slashed simultaneously per event)	Any event involving >1% of active stake simultaneously
ETH at risk in mass slashing scenario post-Pectra (EIP-7251)	Track as effective balance consolidation grows under Pectra
Cost-to-attack estimate (ETH required to acquire 33% of staked supply)	Track directionally; flag if total staked ETH concentration makes acquisition materially cheaper
MEV-Boost OFAC-compliant relay usage (% of blocks)	Any regulatory guidance change that affects compliance threshold

Recommended cadence: Real-time slashing alerts via Beaconcha.in; quarterly review of attack-cost estimates and Pectra consolidation trends.

Dimension 5 Governance Integrity and Change Management

Metric	Monitor For
EIP authorship concentration (top 10 authors as % of implemented Core EIPs)	Any increase above 68% baseline or departure of top-3 authors
ACD call cadence (biweekly calls held vs. scheduled)	Missed calls without explanation; gaps >4 weeks
Hard fork deployment timeline adherence (actual vs. announced activation)	Slippage beyond 90 days from first named target date
COI policy disclosure completeness (% of EF contributors with current disclosures)	Any governance participant without disclosure in force
Testnet failure rate before mainnet activation (testnet failures per upgrade)	Treat >2 testnet failures per upgrade as elevated upgrade risk signal

Recommended cadence: Per-upgrade assessment (triggered by each named fork announcement); annual COI policy review; quarterly EIP authorship concentration check.

Dimension 6 Monitoring, Detection and Incident Communication

Metric	Monitor For
Time-to-detection (hours from incident onset to first documented client team awareness)	For major ICT-related incidents, benchmark against DORA's initial-notification deadline: within four hours of classification as major and no later than 24 hours after the financial entity became aware of the incident [78]
Time-to-external-communication (hours from detection to first public notification)	Track public ecosystem communication separately from regulatory notification. DORA notification is made to the competent authority; client communication is required where clients' financial interests are affected.
Post-mortem publication rate (% of significant incidents with published post-mortem within 30 days)	Compare the institution's internal publication target for significant incidents; DORA's major-incident classification applies to financial entities, not to Ethereum incidents directly, so develop a classification system and monitor against it.
1TS dashboard coverage (controls listed across six dimensions; dated snapshot)	Quarter-on-quarter movement in published control status and coverage

Recommended cadence: Per-incident review; quarterly 1TS dashboard progress review.

Dimension 7 Structured Resilience Testing and Assurance

Metric	Monitor For
Testnet validator scale vs. mainnet (% of mainnet validator count at time of test)	Testnets below 50% of mainnet validator count represent a scale testing gap
Scenario classes covered in current testing cycle (vs. five-class taxonomy in Section 5)	Uncovered scenario classes that have been flagged as significant risks
Structured testing calendar adherence (documented schedule vs. actual exercises)	Absence of a documented schedule (currently the case)
Third-party resilience certifications active (NORS or equivalent)	Number of institutional-grade staking providers with active third-party certification

Metric	Monitor For
Supplementary testing evidence documented by the institution (does not replace DORA TLPT) (internal)	Institutions should maintain use-case-specific scenario libraries as part of their proportionate DORA testing programmes and track performance, risks and mitigations for these programmes. Entities designated for TLPT remain subject to separate requirements determined by a 'competent authority'. Test findings should be classified, prioritised, documented and remediated, with remediation subsequently validated.

Recommended cadence: Per-upgrade assessment; annual certification inventory; ongoing gap analysis for DORA TLPT obligations.

Dimension 8 Transparency, Auditability and Governance Documentation

Metric	Monitor For
EIP lifecycle completeness (% of active EIPs with full revision history, debate record, and ACD decision documented)	Any Core EIP advancing to mainnet without a complete public record
ACD call documentation quality (agendas + notes + recording available per call)	Any call without full documentation within 7 days
Incident post-mortem availability (% of significant events with accessible post-mortem within 60 days)	Gaps for events that meet significance thresholds
1TS report publication cadence	Annual at minimum; quarterly preferred for institutional assurance

Recommended cadence: Automated monitoring of GitHub repositories for documentation gaps; quarterly audit of 1TS publication schedule.

13

Disclaimer & Authors

Disclaimer

This report is an independent research assessment of selected technical and governance characteristics of the Ethereum network as of Tuesday 4th August 2026. It uses certain regulatory and industry frameworks as comparative and analytical reference points only. References to DORA, MiCA, FCA/PRA requirements, US legislation, ISO standards, SOC 2 or other frameworks do not constitute a legal or compliance determination. Such references should not be interpreted as indicating that Ethereum, any participant within the Ethereum ecosystem, or any related product or service complies with, has been certified under, or satisfies the requirements of any applicable law, regulation or supervisory framework. The obligations applicable to any institution will depend on its activities, jurisdiction, regulatory status and manner of using Ethereum.

This report is provided for general informational and research purposes only. It does not constitute legal, regulatory, financial, investment, tax or other professional advice, an offer or solicitation, or a recommendation or endorsement of Ethereum, ETH, any token, financial instrument, service provider or investment strategy. Readers should obtain independent professional advice appropriate to their own circumstances before making any business, investment, operational, regulatory or technology-related decisions.

While reasonable care has been taken in preparing this report, neither the authors nor the publisher make any representation or warranty, express or implied, regarding the accuracy, completeness, adequacy, reliability or timeliness of the information contained herein. Information relating to blockchain networks, digital assets and associated technologies evolves rapidly and may become inaccurate, incomplete or outdated following publication.

To the fullest extent permitted by applicable law, neither the authors, the publisher, nor any of their respective affiliates, directors, officers, employees, agents or advisers shall be liable for any direct, indirect, incidental, consequential, special, exemplary or punitive loss, damage, liability, cost or expense (including any loss of profits, revenue, business opportunities, goodwill or anticipated savings) arising out of or in connection with the use of, reliance upon, or inability to use this report or any information, opinions or conclusions contained herein.

Authors

Swapnil Raj

Head of Innovation

swp@nethermind.io

Dharani Kishore

Head of Product, APAC

dharani.kishore@nethermind.io

Michal Zajac

Chief Strategy Officer

michal@nethermind.io

NETHERMIND

Built at the Foundation of Public Blockchain Networks

www.nethermind.io