

The Normative Theory of Web3 Commercial Integrity

Mohamed ElBendary

July 2025

Abstract

The promise of Web3's decentralized, transparent, and user-owned systems offers transformative potential for global commerce. However, Web3 remains largely inaccessible or intentionally avoided due to user experience friction and persistent risk perceptions. Highly publicized failures over the years point to a fundamental weakness in achieving durable trust required for widespread adoption. This paper introduces a normative theory centered on five interdependent principles, spanning enforcement, trust, duty segregation, governance, and adaptability. Together, they define falsifiable conditions for integrity-by-design Web3 commercial infrastructure. These principles are collectively necessary, though not sufficient, to uphold investor protection, maintain efficient and orderly markets, and ensure transparent capital formation. This framework supports regulators, builders, investors, and institutions with a methodical approach for distinguishing legitimate infrastructure innovations from sophisticated regulatory arbitrage. As major infrastructure decisions accumulate daily, path dependencies continue to entrench brittle architectures. This work aims to chart a socio-technical path to achieving sustainable commercial integrity, thereby broadening access to trustworthy, extensible systems for long-term growth in Web3 commerce.

1. The Promise and the Peril of Web3 Commerce

Web3 technologies have unlocked unprecedented possibilities for innovation in finance (DeFi), digital ownership (NFTs), community governance (DAOs), and beyond. The core tenets of decentralization, on-chain transparency, and composability offer a significant departure from traditional systems often burdened by intermediaries, opacity, and restricted access. Yet this emerging landscape carries serious risks. Rug pulls, protocol exploits, governance opacity, and unstable market mechanics have eroded trust and hindered broader adoption. Beyond DeFi, all Web3 use cases share a need for principled, integrity-first socio-technical design. If Web3 is to mature into a resilient global commercial layer, more than innovative code is required.

As institutional engagement and regulatory scrutiny increase, the opportunity to embed robust commercial integrity at the infrastructure level is narrowing. Recent regulatory actions underscore this urgency. In May 2025, the Monetary Authority of Singapore ordered all local digital token service providers to cease offering services to overseas clients unless licensed, with compliance required by June 30. Around the same time, Thailand's Securities and Exchange Commission moved to block access to major global exchanges including Bybit, OKX,

and CoinEx, citing unlicensed operations. These enforcement decisions targeted platforms with large user bases and cross-border reach, illustrating how the absence of aligned infrastructure standards can trigger sweeping restrictions and market turbulence. Without clear commercial integrity frameworks, institutions and regulators alike face mounting challenges in evaluating and trusting emerging Web3 infrastructure, causing continued delay in adoption and increasing systemic friction.

How do we ensure that these new commercial environments are not just technologically novel, but also fair, legitimate, orderly, and protective of all participants? We propose that a set of system-level socio-technical architectural principles, intentionally embedded at design time, can deliver these outcomes. Doing so will require a shift away from ad hoc and reactive solutions toward comprehensive, multi-stakeholder integrity-by-design frameworks.

2. The Normative Theory of Web3 Commercial Integrity

This paper presents a normative theory composed of five prescriptive principles that together define the essential conditions for robust commercial integrity in Web3 systems.

Definition: A commercial environment is any socio-technical system that enables value exchange between independent participants.

Theory statement:

For any Web3 system operated in a commercial environment, the environment provides:

a. investor protection, b. efficient, fair, legitimate, and orderly (i.e. risk-controlled) markets, and c. systemic, transparent, and global capital formation *only if* the following conditions are met:

1. **Atomic On-Chain Rule Enforcement:** All applicable compliance rules are enforced on-chain atomically within each transaction context.

Hypothesis: If a system enforces all compliance logic atomically at the transaction level, then it will not exhibit execution-path-dependent violations (e.g., partial compliance, regulatory arbitrage).

Falsification Criteria: Empirical evidence of regulatory rule violations or investor harm in a system with full atomic enforcement would refute this proposition.

2. **Primacy of On-Chain Trust Assessment:** Assessment of trustworthiness of market participants is primarily derived from on-chain rule enforcement and on-chain reputation.

Hypothesis: Systems where on-chain reputation scores and rule adherence histories are the primary basis of trust will outperform off-chain-based systems in fraud mitigation and capital cost reduction.

Falsification Criteria: If off-chain identity-reliant systems outperform on-chain-reputation-first systems on fraud incidence or capital efficiency, the proposition is falsified.

- 3. On-Chain Segregation of Duties:** Segregation of duties is maintained on-chain (e.g., through use of cross-contract attestations): regulator/compliance functions, protocol developers, auditors, RegTech developers, and app builders must have distinct, verifiable identities (e.g., smart contract addresses, ENS names) with no controlling stake or undue influence of one over any of the others.

Hypothesis: Systems with verifiable separation between protocol developers, auditors, governance agents, and compliance modules will exhibit fewer governance failures than systems without enforced separation.

Falsification Criteria: If verifiably segregated systems demonstrate equal or greater governance failure than non-segregated systems (e.g., protocol capture, rug pulls), the proposition is refuted.

- 4. Modular and Scoped Stakeholder Governance:** Governance is modular down to the contract/liquidity pool level, appropriately scoped by stakeholders directly involved in a commercial activity, and can be tiered with mechanisms like weighted voting or role-based permissions.

Hypothesis: When governance rights are scoped to stakeholders with direct exposure to system components, governance outcomes will have higher participation rates and better alignment.

Falsification Criteria: If scoped systems show lower participation, greater voter apathy, or misaligned policy outcomes versus centralized governance structures, this pillar is disproved.

- 5. Adaptable Governance without Market Disruption:** Governance mechanisms allow for approved rule changes and emergency fixes to be applied without breaking the underlying market infrastructure or causing undue interruption to ongoing commercial activities.

Hypothesis: Systems using phased governance, timelocks, and modular

upgrades will adapt to market/regulatory change without increasing operational downtime or volatility.

Falsification Criteria: If such systems face equal or greater market disruption than non-adaptable systems during protocol changes, this proposition fails.

These five conditions are interdependent requirements derived from analysis of commercial integrity failures in existing Web3 systems and the structural needs of institutional adoption. The necessity of all five conditions derive from their coverage of functionally distinct failure modes and the dependence of the system's integrity properties on each of these conditions:

- **Execution integrity:** ensured by *atomic on-chain compliance enforcement*, which is required to uphold investor protection and to sustain fair, orderly, and efficient markets.
- **Participant accountability:** enabled by *on-chain trust assessment primacy*, which is likewise essential for investor protection and market fairness.
- **Governance safety:** maintained through *on-chain segregation of duties* and *modular, scoped governance*, both of which are necessary for investor protection and for market integrity across decentralized ecosystems and jurisdictions.
- **Evolvability under uncertainty:** supported by *regulatory adaptability without market disruption*, which is critical for preserving investor protection, maintaining market continuity, and enabling systemic capital formation.

Each condition protects against a unique systemic threat. Therefore:

Absent any one of these conditions, a Web3 system lacks sufficient safeguards to credibly claim robust commercial integrity.

While specific implementations may vary, the principles themselves are universally necessary for any credible commercial system operating without centralized intermediaries.

3. Operationalizing the Five Pillars: Design Implications and Illustrative Justifications

To support institutional adoption and regulatory alignment, this section presents the practical rationale and design relevance of each of the five conditions for Web3 commercial integrity. It outlines their architectural implications and highlights real-world failure patterns that each principle is intended to mitigate. Prior work on on-chain policy orchestration in Uniswap v4 (ElBendary, 2025) offers an illustrative application of these five pillars within the decentralized finance (DeFi) context.

Pillar 1: Atomic On-Chain Rule Enforcement

What it means: Rules governing trade execution and applicable compliance requirements such as Know Your Customer (KYC), sanctions screening, or transaction limits must be executed within a single, indivisible on-chain transaction. This includes integration with external attestations (e.g. Quadrata attributes for KYC) or data sources when needed. If any rule fails, the entire transaction must revert, ensuring full compliance integrity across protocol boundaries.

Why it's crucial: This mechanism ensures that compliance is automatic, consistent, and tamper-proof. It prevents execution-path-dependent violations (e.g., rule circumvention during multi-protocol operations), enforces jurisdictional controls, and removes reliance on off-chain or manual compliance interventions. It directly supports investor protection and fair, orderly, and efficient markets. This enforcement must apply consistently across all interactions, protocols, and jurisdictions.

Illustrative Gap:

Cross-border Web3 transactions often rely on fragmented or incomplete KYC workflows. Multi-step DeFi interactions (e.g., combining borrowing, liquidity provision, and leverage) may appear compliant in isolation but violate exposure or jurisdictional constraints when executed together. Atomic rule enforcement eliminates these partial-compliance risks.

Pillar 2: Primacy of On-Chain Trust Assessment

What it means: Trust in a market participant, whether an individual, protocol, or organization, must primarily be based on their verifiable on-chain history. This includes adherence to enforceable rules, transaction behavior, governance participation, and the security performance of contracts they deploy or interact with. While off-chain information can provide valuable context, it is not a sufficient substitute for persistent, transparent on-chain performance when assessing risk.

Why it's crucial: In globally distributed and pseudonymous systems, on-chain trust mechanisms reduce fraud, mitigate information asymmetry, and minimize reliance on unverifiable or reputation-based credentials. While privacy-preserving technologies remain essential, commercial integrity also requires adequate transparency for counterparties to assess trustworthiness and for regulators to monitor systemic risk. This principle supports investor protection and fair market access by reconciling selective confidentiality with traceable accountability. Importantly, the model does not require full de-anonymization, but it does require that pseudonymous actors be linkable to accountable entities under well-defined governance conditions.

Illustrative Gap:

Fraud-prone token launches and exploit-prone DAOs often attract off-chain attention while lacking any verifiable on-chain trust profile. Without a formal reputation layer, actors are

evaluated through social signals rather than performance metrics. On-chain reputation systems would enable a shift from personality-based trust to protocol-based accountability, aligning incentives and reducing institutional onboarding risk.

Pillar 3: On-Chain Segregation of Duties

What it means: Web3 systems must enforce structural separation between critical functions including protocol development, governance operations, auditing, compliance infrastructure, and application development. Each role should be associated with a verifiable and independent on-chain identity, supported by attestation mechanisms and iterative ownership mapping. Where token-based governance is used, systems must detect and mitigate recursive control structures or hidden influence across domains. Empirical research confirms that complex token distributions often conceal concentrated control despite formal decentralization (Nadler & Schär, 2021).

Why it's crucial: Unchecked concentration of authority across functional roles enables self-dealing, regulatory arbitrage, and protocol capture. Segregating duties is essential for creating resilient governance structures that protect against insider risk and ensure system-wide accountability. A recent example is hook contract implementing the Time-Weighted AMM (TWAMM) for Uniswap v4, demonstrated best practice role separation: Paradigm produced the research, FWB DAO governed deployment decisions, Uniswap Labs provided infrastructure, Zaha Studio provided the implementation, and independent auditors performed security verification. This model enabled sophisticated treasury management capabilities while preserving trust and technical integrity.

Illustrative gap: Role conflicts have historically undermined trust in both traditional and decentralized systems. Examples include protocol teams controlling their own governance votes, auditors financially entangled with development teams, or compliance verifiers directly benefiting from approval decisions. These patterns mirror structural conflicts in traditional finance such as custodians acting as traders or underwriters reviewing their own products. Without enforced duty segregation, such arrangements invite front-running, market manipulation, and audit failures. Conversely, research shows that well-structured decentralized exchanges with proper separation of responsibilities can achieve market quality on par with centralized venues (Barbon & Ranaldo, 2024).

Pillar 4: Modular and Scoped Stakeholder Governance

What it means: Web3 governance must be modular with explicit boundaries defined at the contract (e.g. policy-enforcement contract) or functional unit (e.g. DeFi pool) level, and scoped to stakeholders with direct economic, technical, or compliance exposure to a component's outcomes. Effective implementations include tiered voting, domain-specific permissions, and role-restricted authority, ensuring that only relevant actors influence applicable decisions. Governance frameworks must support opt-in participation, allowing users to delegate, abstain, or exit from decisions unrelated to their operational or risk surface. Empirical research on DeFi

lending protocols confirms that scoped governance improves interest rate discovery, reduces policy volatility, and enhances liquidity provision without compromising market integrity (Zhang et al., 2023).

Why it's crucial: Web3 protocols operate across asset classes, jurisdictions, and user verticals. Monolithic, one-token-one-vote systems enable cartelization, discourage participation, and produce misaligned outcomes, especially when voters lack direct exposure to the affected domain. In contrast, modular, scoped governance narrows the range of each decision's effect, aligns authority with responsibility, and supports safe, parallel experimentation. For institutional actors, it reduces governance risk, clarifies control boundaries, and enables targeted due diligence across protocol layers.

Illustrative gap: Existing research confirms that governance architecture significantly impacts protocol sustainability and user protection (Siriwardana et al., 2023). However, many systems allow global token holders to vote on highly localized or technical issues, such as adjustment of fee parameters in jurisdiction-specific pools or deployment of application-specific modules, leading to voter apathy, misalignment, and incentive-driven manipulation.

A recent framework demonstrates a viable alternative. In the on-chain policy orchestration model for Uniswap v4 (EIBendary, 2025), governance is modularized at the liquidity pool level. Scoped governance applies only to policy-specific contracts (hooks) attached to a given pool, while the core protocol is governed separately under a protocol-wide governance structure. This decoupled model aligns governance authority with risk exposure and illustrates a replicable template for scoped stakeholder governance in complex, multi-domain DeFi ecosystems.

Pillar 5: Governance Adaptability Under Regulatory and Market Volatility

What it means: Web3 systems must evolve through economic environment changes, security patches, and regulatory updates while remaining composable, without breaking integrations, or triggering market-wide halts. Governance must support modular upgrades, parameter adjustments, and emergency mitigations through mechanisms such as timelocks, upgradeable proxies, scoped change domains, and contract versioning. Crucially, adaptability must be anticipatory and intentionally designed for, not reactive or ad hoc, ensuring uninterrupted market function, legal compliance, and protocol integrity across evolving conditions.

Why it's crucial: Markets do not wait for codebase consensus. Legal obligations shift, security threats emerge, and user needs evolve. Systems that cannot adapt without forks, freezes, or coordination breakdowns become brittle and untrustworthy. For institutions, adaptability is not optional as it underpins operational compliance, auditability, and investor confidence. Orderly, pre-authorized evolution requires governance envelopes, structured upgrade windows, and stakeholder-aligned rollout paths to minimize systemic risk during transition periods and enable sustained engagement.

Fast-moving protocols often optimize for user acquisition or feature velocity at the expense of long-term flexibility, often to capture first-mover advantage or market share. This creates brittle path dependencies where early architectural choices become barriers to regulatory responsiveness or security upgrades. Governance adaptability must be embedded from inception, not retrofitted after scale.

Illustrative gap: Historical examples reveal not a simple lack of technical flexibility, but the deep structural challenges of evolving Web3 systems under pressure.

The 2016 Ethereum DAO fork shows that even when procedural adaptation succeeds, the absence of predefined governance mechanisms can fracture community consensus. Faced with a devastating smart contract exploit, the Ethereum community implemented a hard fork to reverse the theft, choosing to prioritize investor protection over the “code is law” ethos. Although 87% of voting ETH supported the rollback, fewer than 6% of the total ETH supply participated, leading to the permanent creation of Ethereum Classic. This episode underscores the cost of post hoc adaptation without clear preauthorized governance envelopes manifested as community division, interpretive ambiguity, and reputational strain.

Similarly, the 2022 Tornado Cash sanctions (later overturned by a U.S. federal appeals court in 2024) revealed how protocol immutability can collide with dynamic regulatory expectations. The court ruled that immutable smart contracts could not be classified as “property” subject to Treasury Department authority, and the sanctions were lifted in early 2025. This wasn’t a failure of rigidity per se, but rather a failure of regulatory fit because Tornado Cash had no governance mechanism or upgrade path capable of mediating between compliance requests and protocol function. The Tornado Cash case illustrates that legal adaptability must be engineered even when technical finality appears secure.

In both cases, the core issue was not that change was impossible, rather that change lacked procedural clarity, formal scope, or systemic containment. These cases underscore the need for anticipatory, domain-bounded adaptability where systems evolve within known guardrails that preserve composability, protect market continuity, and allow for policy-aligned upgrades without fracturing user trust or governance legitimacy. Adaptability, in this sense, is a systemic capability for commercial legitimacy in volatile legal and operational environments.

These five conditions form an interdependent set of socio-technical constraints necessary to embed, by design, credible commercial integrity in Web3 systems. In their absence, systems revert to off-chain enforcement, centralized chokepoints, or structural compromises that erode the transparency, fairness, and reliability required for durable institutional participation and regulatory legitimacy. Applied together, they offer a systematic foundation for Web3 infrastructure that aligns technological innovation with the fiduciary and legal standards of real-world commerce. They also form the basis for commercial integrity assessment frameworks applicable to both emerging architectures and existing systems.

5. Evaluation Rubric: Assessing Commercial Integrity in Web3 Systems

This rubric transforms the five-pillar framework into a set of evaluative criteria for systematically assessing existing and proposed Web3 infrastructure. It enables stakeholders to move beyond surface metrics and evaluate whether a system is architecturally capable of sustaining commercial integrity under regulatory, market, and operational stress.

Each criterion is aligned with a design pillar and rated across three dimensions:

Pillar	Key Evaluation Criteria	Sample Indicators
1. Atomic Rule Enforcement	Can compliance, risk, and execution rules be enforced atomically within transaction boundaries?	<ul style="list-style-type: none"> - Use of pre-trade validation logic - On-chain approvals tied to transfer - Rejection of non-compliant transactions without fallback logic
2. On-Chain Trust Assessment	Can participant trustworthiness be evaluated through verifiable on-chain evidence, not off-chain heuristics?	<ul style="list-style-type: none"> - Attestation registries - On-chain reputation metrics - Traceable disclosures to accountable entities tied to addresses
3. Segregation of Duties	Are roles (developer, auditor, regulator interface) clearly separated on-chain with no shared control domains?	<ul style="list-style-type: none"> - Distinct governance keys - Role-restricted modules - Contract-level authority mapping
4. Scoped Stakeholder Governance	Are governance rights modularized and scoped to stakeholders exposed to the governed domain's risks?	<ul style="list-style-type: none"> - Pool-level governance - Tiered vote weight by role - Opt-in delegation models
5. Governance & Regulatory Adaptability	Can the system evolve—securely and legally—without halting markets or fracturing consensus?	<ul style="list-style-type: none"> - Timelocked upgrades - Upgradeable proxy architectures - Scoped upgrade domains with rollback plans

Supplementary Assessment Dimensions

Including the following architectural dimensions provides deeper visibility during due diligence:

Dimension	Key Questions
Governance Concentration	Are voting rights disproportionately concentrated (e.g., through staking derivatives, delegation)?
Operational Resilience	Can the system maintain integrity during security events, off-chain outages, or market volatility?
Composability Preservation	Do upgrades or policy changes avoid breaking integrations or dependencies?
Investor Protection Continuity	Are users shielded from unvetted upgrades, unverified protocols, or policy opacity?
Regulatory Readiness	Can the system transparently demonstrate compliance capacity under evolving legal regimes?

Application Scenarios

Use Case	How to Apply This Rubric
Protocol Design Review	Embed criteria as a checklist during architecture, testnet, and audit phases.
Institutional Due Diligence	Score candidate systems across each pillar pre-allocation or integration.
Regulatory Evaluation	Shift from outcome-based assessments to architectural capacity analysis.
Grant or Ecosystem Funding	Use rubric to vet foundational integrity before capital deployment.

Systematic commercial integrity assessment transforms Web3 from experimental chaos to institutional-grade infrastructure. When the five pillars are treated as evaluation criteria, not just as design goals, they create a shared domain-specific language for policy alignment, institutional trust, and ecosystem resilience.

6. Strategic Implications and the Cost of Delay

Adopting the Normative Theory of Web3 Commercial Integrity as a design philosophy has profound implications:

- **For Builders:** This theory provides clear architectural principles for building commercially viable Web3 systems. While early adoption may create short-term competitive disadvantages, these principles are essential for long-term viability. Systems that compromise on foundational capabilities face devastating risks as they scale. For example, systems built without regulatory adaptability automatically create an uncertainty tax that slows adoption, limits institutional participation, and exposes teams to competitive pressure from more flexible alternatives.
- **For Investors & Users:** It offers a framework of testable conditions for evaluating the integrity of Web3 projects and making more informed participation decisions.
- **For the Ecosystem:** It fosters an environment where capital is more likely to flow towards well-governed, secure, and fair systems, accelerating maturation and adoption.
- **For Regulators:** It demonstrates pathways for achieving regulatory goals through technologically native means, potentially informing future dialogue.

6.1. The Cost of Delayed Action

Current market conditions provide compelling evidence for this theory's urgency. User experience problems persist across DeFi as users are forced to manually manage complex token approval workflows, creating false trade-offs between security and functionality that proper commercial integrity architecture would eliminate. These UX failures, evidenced by widespread community discussions about approval management, represent systematic investor protection failures that sophisticated architectural frameworks could prevent.

Meanwhile, institutional capital remains largely sidelined by regulatory uncertainty. Regulatory guidance is evolving toward frameworks that can accommodate technology-native approaches to commercial integrity (Financial Conduct Authority, 2024; Securities and Exchange Commission, 2024). The UK's FCA, for example, is seeking input on stablecoin frameworks while maintaining an innovation-friendly stance (Financial Conduct Authority, 2025), showing regulatory willingness to engage. However, without systematic commercial integrity standards, institutions cannot distinguish legitimate infrastructure from sophisticated regulatory arbitrage.

This causes the entire ecosystem to bear an "uncertainty tax" that slows adoption and innovation across the ecosystem.

Recent security incidents further demonstrate these systematic risks. Despite Hyperliquid's technical sophistication and \$1.57B TVL, users recently lost funds through phishing attacks that exploited the gap between off-chain website verification and on-chain transaction execution, illustrating broader DeFi security challenges documented in systematic literature reviews (Wang et al., 2024). The incident revealed how current Web3 systems force users to manually verify website authenticity and understand complex transaction contexts. Proper trust assessment mechanisms and on-chain rule enforcement would prevent this kind of systematic vulnerability because enforcement is not dependent on a particular frontend. These failures create additional uncertainty costs beyond regulatory concerns, showing how architectural gaps undermine investor protection even in technically advanced platforms.

Historical precedent demonstrates the compounding of infrastructure compromises. The 1970s 'paperwork crisis' forced adoption of intermediated clearing systems designed as temporary solutions until better technology emerged (Le & Campbell, 2025). Despite decades of technological advancement that could enable direct ownership and instant settlement, the intermediated system persists because of locked in legacy choices creating significant political will inertia for change. Today's Web3 infrastructure decisions face the same dynamics where successful deployments create precedents that make architectural improvements exponentially more difficult and expensive as adoption scales.

The systematic gaming of user metrics further demonstrates these integrity gaps. As one project founder recently revealed, Web3 projects routinely inflate user numbers through farming operations that extract value without genuine participation, with some 'users' generating less than \$1 despite being counted in the hundreds of thousands. This gaming corrupts investment decisions, undermines authentic projects, and degrades trust across the ecosystem. Again, proper on-chain trust assessment and atomic rule enforcement would prevent such failed signaling.

Empirical governance analysis reveals these risks are already systemic. Research shows that even after accounting for complex pooling and staking arrangements, most DeFi tokens remain concentrated among small groups of holders, creating the potential for coordinated governance capture (Nadler & Schär, 2021). This concentration persists despite protocols' decentralized technical architectures, demonstrating that governance integrity cannot be assumed from technical sophistication alone.

These systematic vulnerabilities align with regulatory assessments identifying governance concentration and operational resilience as key risks in decentralized finance (U.S. Department of the Treasury, 2024; Financial Stability Board, 2023).

6.2. The Path Forward

Moving forward requires immediate, coordinated action from all stakeholders. Real-time evidence demonstrates this urgency as major institutional infrastructure decisions are being made without proper commercial integrity frameworks, globally.

Kazakhstan announced "CryptoCity" where cryptocurrency will be used for "purchasing goods, services, and even beyond" (Zmudzinski, 2025). How do we evaluate a comprehensive crypto economy requiring robust commercial integrity but being planned and actively built without apparent systematic integrity-first principles? The app-first blockchain strategy, exemplified by platforms like Abstract Chain with 2.01 million users and Hyperliquid with \$1.57B TVL, is creating path dependencies where successful applications lock in potentially problematic architectural choices before proper frameworks are available.

Consider the cascading implications of institutional RWA integration proceeding using infrastructure that cannot deliver promised compliance capabilities, stablecoin networks launching without addressing fundamental monetary integration challenges, or new L1s prioritizing user growth over regulatory adaptability. Each successful deployment without proper commercial integrity creates precedents that make later architectural improvements exponentially more difficult and expensive.

This theory provides the foundation, but realizing its potential demands collaborative implementation between builders, regulators, and institutions before current market dynamics lock in suboptimal approaches. The choice before us is clear: build Web3 infrastructure on integrity by design, or risk fragmenting its transformative potential through ad hoc approaches that satisfy no one's long-term interests.

7. Conclusion: Building the Future of Commerce on Integrity

Web3 stands at a critical juncture. As institutional capital waits on the sidelines, regulatory frameworks crystallize globally, and infrastructure decisions compound daily, the choices made now will determine whether decentralized systems fulfill their promise of more equitable, transparent, and efficient global commerce.

The Normative Theory of Web3 Commercial Integrity offers a clear architectural foundation and an actionable evaluation framework for aligning innovation with fiduciary, regulatory, and operational standards. The five pillars of atomic rule enforcement, on-chain trust assessment, segregation of duties, scoped governance, and adaptable systems, together equip stakeholders with rigorous criteria to differentiate genuine infrastructure from sophisticated regulatory arbitrage.

Ad hoc architectures, even in billion-dollar protocols, continue to produce avoidable failures that

directly undermine investor protection, compromise security, and cause capital misallocation. Regulatory uncertainty persists not because technology is immature, but because integrity is inconsistently implemented. Infrastructure decisions today will shape market outcomes for years. The cost of retrofitting governance, compliance, and risk safeguards after scale is no longer marginal.

This theory defines the path. Realizing it demands a coordinated shift by all stakeholders including builders embedding integrity by design, institutions adopting systematic assessment criteria, and regulators moving beyond technology-oblivious compliance checklists toward proactive, architecture-aware oversight leveraging technological realities.

The window for systematic action remains open. What we build now will determine what is ultimately possible in Web3 relative to its ethos of globally fair, accessible, and durable value exchange.

References

Adams, H., McCarthy, D., & White, D. (2021). TWAMM. *Paradigm*.
<https://www.paradigm.xyz/2021/07/twamm>

Adams, H., Zinsmeister, N., Salem, M., Keefer, R., & Robinson, D. (2022). Uniswap v3 Core. *Uniswap Foundation*. <https://uniswap.org/whitepaper-v3.pdf>

Adams, H., Zinsmeister, N., & Robinson, D. (2024). Uniswap v4: Hooks and the Future of DEX Innovation. *Uniswap Foundation*. <https://blog.uniswap.org/uniswap-v4>

Atkins, P. (2025, May). Remarks at SEC Speaks 2025. *U.S. Securities and Exchange Commission*. Washington, D.C.

Barbon, A., & Rinaldo, A. (2024). On the Quality of Cryptocurrency Markets: Centralized versus Decentralized Exchanges. *Journal of Financial Economics*, 153, 103-134.

Broner, S. (2025, June 4). How stablecoins become money: Liquidity, sovereignty, and credit. a16zcrypto. <https://a16zcrypto.com/posts/article/how-stablecoins-become-money/>

Capponi, A., Jia, R., & Wang, J. (2023). Decentralized Exchange Protocols and Market Structure. *Annual Review of Financial Economics*, 15, 153-181.

EIBendary, M. (2025). Uniswap Protocol V4 Hook-based On-Chain Policy Orchestration Architecture. GitHub. <https://github.com/mbelbendary/uniswap-v4-hook-manager-framework>

Financial Conduct Authority. (2024). Guidance on Cryptoasset Financial Promotions. *FCA Policy Statement PS24/6*. London: FCA.

Financial Conduct Authority. (2025, May 28). FCA seeks further views on stablecoins and crypto custody. Financial Conduct Authority.

Financial Stability Board. (2023). DeFi Report: Financial Stability Risks and Regulation. Basel: FSB.

Friends with Benefits. (2025, June 5). Redesigning the FWB Token System. <https://www.fwb.help/stories/redesigning-the-fwb-token-system>

Gudgeon, L., Moreno-Sanchez, P., Roos, S., McCorry, P., & Gervais, A. (2020). SoK: Layer-Two Blockchain Protocols. *Proceedings of the 24th International Conference on Financial Cryptography and Data Security*, 201-226.

Jennings, M. (2025, June 2). The end of the foundation era in crypto. a16zcrypto. <https://a16zcrypto.com/posts/article/end-foundation-era-crypto/>

Jensen, J. R., von Wachter, V., & Ross, O. (2021). An Introduction to Decentralized Finance (DeFi). *Complex Systems Informatics and Modeling Quarterly*, 26, 46-54.

Le, T., & Campbell, A. (2025). Crypto and the Evolution of the Capital Markets. SSRN.

Lehar, A., & Parlour, C. A. (2023). Decentralized Exchange Mechanisms and Token Economics. *Review of Finance*, 27(4), 1445-1487.

Milionis, J., Moallemi, C. C., Roughgarden, T., & Zhang, A. L. (2023). Automated Market Making and Loss-Versus-Rebalancing. *Proceedings of the 2023 ACM Conference on Economics and Computation*, 1178-1179.

Monetary Authority of Singapore. (2025, May 15). Notice on Cessation of Digital Payment Token Services to Overseas Persons. *MAS Notice DPT-N01*. Singapore: MAS.

Nadler, M., & Schär, F. (2021). Decentralized Finance, Centralized Ownership? An Iterative Mapping Process to Measure the Level of Decentralization in the DeFi Ecosystem. *University of Basel Working Paper*.

Park, A. (2023). The Conceptual Flaws of Constant Product Automated Market Making. *Management Science*, 69(11), 6944-6952.

Qin, K., Zhou, L., & Gervais, A. (2022). Quantifying Blockchain Extractable Value: How Dark is the Forest? *Proceedings of the 2022 IEEE Symposium on Security and Privacy*, 198-214.

Securities and Exchange Commission. (2024). Framework for "Investment Contract" Analysis of Digital Assets. *SEC Staff Legal Bulletin No. 19*. Washington, D.C.: SEC.

Siriwardana, J., Kaluarachchi, A., & Nanayakkara, S. (2023). A Systematic Review of Governance in Decentralized Finance. *IEEE Access*, 11, 42953-42968.

U.S. Department of the Treasury. (2024). DeFi Illicit Finance Risk Assessment. *Treasury Financial Crimes Enforcement Network*. Washington, D.C.: FinCEN.

Wang, Y., Chen, T., Li, X., & Zhang, X. (2024). DeFi Security: A Systematic Literature Review of Vulnerabilities in Decentralized Finance. *Computers & Security*, 139, 103-118.

Werner, S. M., Perez, D., Gudgeon, L., Klages-Mundt, A., Harz, D., & Knottenbelt, W. J. (2022). SoK: Decentralized Finance (DeFi). *Proceedings of the 4th ACM Conference on Advances in Financial Technologies*, 30-46.

Xu, J., Paruch, K., Cousaert, S., & Feng, Y. (2023). SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) protocols. *ACM Computing Surveys*, 55(11), 1-50.

Zhang, Y., Chen, X., & Park, D. (2023). DeFi Protocols for Loanable Funds: Interest Rates, Liquidity and Market Efficiency. *European Financial Management*, 29(4), 1235-1267.

Zhou, L., Qin, K., Torres, C. F., Le, D. V., & Gervais, A. (2021). High-Frequency Trading on Decentralized On-Chain Exchanges. *Proceedings of the 2021 IEEE Symposium on Security and Privacy*, 428-445.

Zmudzinski, A. (2025, May 30). Thailand to block Bybit, OKX and other crypto exchanges on June 28. Cointelegraph.

<https://cointelegraph.com/news/thailand-blocks-okx-bybit-crypto-exchanges>

Zmudzinski, A. (2025, May 29). Kazakhstan to launch crypto pilot zone for payments and adoption. Cointelegraph.

<https://cointelegraph.com/news/kazakhstan-pilots-cryptocurrency-crypto-payments-adoption>