The Normative Theory of Web3 Commercial Integrity

By Mohamed ElBendary

Date: June 7, 2025

Abstract

The promise of Web3—decentralized, transparent, and user-owned systems—offers transformative potential for global commerce. Yet as institutional adoption accelerates and regulatory frameworks crystallize, the opportunity to embed robust commercial integrity architectures is closing fast. This paper introduces "The Normative Theory of Web3 Commercial Integrity," a systematic framework providing both design principles for builders and assessment criteria for evaluating existing systems. The theory identifies five architectural conditions that are collectively necessary for Web3 systems to provide genuine investor protection, efficient markets, and transparent capital formation. Unlike ad hoc approaches, this framework helps stakeholders distinguish legitimate infrastructure innovations from sophisticated regulatory arbitrage. As major infrastructure decisions accumulate daily, the theory offers essential tools for regulators, builders, investors, and institutions navigating the transition to sustainable Web3 commercial infrastructure.

Why Web3, Not Just DeFi?

While decentralized finance (DeFi) represents the most mature and visible application of Web3 commercial systems today, the scope of this normative theory extends far beyond financial protocols. Web3 is fundamentally transforming how value is exchanged across multiple domains:

Emerging Commercial Ecosystems: NFT marketplaces facilitate billions in digital asset trading. Tokenized real-world assets (RWAs) are bringing traditional securities, commodities, and real estate on-chain. Sovereign asset tokenization now makes it possible to trade oil, natural gas, and agricultural commodities on-chain, fundamentally transforming how these critical resources are exchanged. Gaming economies enable complex virtual asset exchanges. Creator platforms monetize content through tokenized engagement. Decentralized autonomous organizations (DAOs) coordinate economic activity across industries—from venture capital to supply chain management.

Convergent Infrastructure Needs: These diverse applications share common commercial integrity requirements. Whether trading tokens on a DEX, purchasing NFTs, investing in tokenized real estate, or contributing to a DAO treasury, users require consistent investor protection, fair market mechanisms, and transparent capital formation. The same architectural

principles that enable trust in DeFi—atomic rule enforcement, verifiable reputation, segregated duties, appropriate governance, and adaptability—are just as essential for NFT authenticity, RWA compliance, gaming asset integrity, and DAO governance.

Future-Proofing Regulatory Frameworks: As Web3 evolves into new domains—from AI model marketplaces to carbon credit trading and decentralized physical infrastructure—regulatory approaches must be grounded in universal commercial integrity principles, not application-specific rules. A normative theory limited to DeFi would quickly become obsolete as new Web3 applications emerge.

Network Effects and Composability: Web3's composable nature allows DeFi protocols to interact seamlessly with NFT platforms, RWA tokenization systems, and DAO governance mechanisms within unified user workflows. Analysis of decentralized exchange protocols shows that these market structure innovations require systematic commercial integrity approaches to achieve their full benefits (Capponi et al., 2023; Lehar & Parlour, 2023). Commercial integrity cannot be achieved in isolated silos—it requires approaches that work consistently across the entire Web3 landscape.

Regulatory Vision Alignment: This comprehensive approach supports the Super-App vision articulated by SEC Chairman Paul Atkins in May 2025—a single portal for trading securities and non-securities. Such a unified platform requires precisely the systematic commercial integrity architecture described in this theory, ensuring consistent investor protection and market integrity across all asset classes and transaction types.

This theory offers foundational architectural principles for any socio-technical system that enables value exchange between independent participants. As Web3 commerce expands, these principles help ensure that robust commercial integrity scales with it.

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 departure from traditional systems often burdened by intermediaries, opacity, and restricted access.

Yet this nascent landscape is not without peril. Rug pulls, protocol exploits, volatile markets, and opaque governance have eroded trust and hindered broader adoption. For Web3 to mature into a reliable global commercial layer, more than innovative code is needed; we require principled, integrity-first socio-technical design. As Web3 scales toward institutional adoption and regulatory scrutiny, the opportunity to embed proper commercial integrity is closing fast.

Recent regulatory actions illustrate this urgency. In May 2025, Singapore ordered local crypto firms to cease overseas operations by June 30 (Monetary Authority of Singapore, 2025), while

Thailand simultaneously blocked major exchanges including Bybit and OKX, citing unlicensed operations (Zmudzinski, 2025). These regulatory responses, affecting billions in trading volume, demonstrate how current fragmented approaches create sudden market disruptions. Meanwhile, the absence of standardized commercial integrity frameworks makes it difficult for institutions to evaluate competing infrastructure approaches consistently, creating uncertainty that slows adoption across the ecosystem.

The problems of today's financial system are not accidental—they stem from "temporary" technological compromises that became permanent. In the 1960s, surging trading volume overwhelmed manual paper certificate processing, prompting regulators to implement intermediated clearing as an emergency measure. As one analysis notes, what was meant as "an interim step on the way to a certificateless society became the permanent basis of U.S. securities settlement" (Le & Campbell, 2025). This historical pattern—where urgent infrastructure decisions create decades-long path dependencies—shows why commercial integrity architecture must be built correctly from the foundation, not retrofitted later.

How do we ensure that these new commercial environments are not just technologically novel, but also enduringly fair, legitimate, orderly, and protective of all participants? We propose that systematic architectural principles can achieve these outcomes, though doing so requires moving beyond ad-hoc and retrofitted solutions to comprehensive integrity-by-design frameworks.

2. The Normative Theory of Web3 Commercial Integrity

This paper presents a normative theory—a set of prescriptive principles—defining 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.

The theory states:

> 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.

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.
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.
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.
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.

These five conditions are interdependent architectural requirements derived from analysis of commercial integrity failures in existing Web3 systems and the structural needs of institutional adoption.

3. Deconstructing the Five Pillars of Web3 Commercial Integrity

Let's explore why each of these five conditions is critical:

Pillar 1: Atomic On-Chain Rule Enforcement

What it means: Rules governing interactions—from trade execution to compliance checks (e.g., KYC/AML attestations, if applicable)—are not just written down but are executed by the blockchain itself, including integration with verified external data sources when needed. Compliance code executes within a single, indivisible transaction boundary. If any rule fails, the entire transaction reverts. This enforcement must apply consistently across all interactions, protocols, and jurisdictions.

Why it's crucial: This ensures that rules are applied consistently and predictably, with no possibility of partial execution or manipulation of intermediate states. Even in complex scenarios involving multiple protocol interactions in a single transaction (such as flash accounting in AMM protocols), atomic enforcement applies to each component interaction. Automated enforcement of predefined compliance logic ensures consistent rule application across jurisdictions, without relying on manual oversight or trust in intermediaries. This forms the basis for investor protection and orderly markets.

Current compliance gaps illustrate this necessity. Cross-border transactions often rely on manual KYC verification, which can be bypassed or only partially completed, creating regulatory arbitrage opportunities. Multi-step DeFi transactions—such as lending, swapping, and yield farming—may comply with rules at individual steps while violating aggregate exposure limits. Atomic enforcement would ensure that all applicable compliance rules—from sanctions screening to transaction limits to accreditation requirements—are verified atomically before any transaction execution, preventing partial compliance or rule circumvention.

Pillar 2: Primacy of On-Chain Trust Assessment

What it means: While off-chain information can provide context, the core basis for trusting a participant (be it an individual, a DAO, or a protocol) comes from their verifiable on-chain history—their adherence to rules, their transaction patterns, their governance participation, and the security track record of contracts they deploy or interact with.

Why it's crucial: In pseudonymous, globally distributed environments, on-chain reputation provides the most reliable and verifiable foundation for trust assessment, directly supporting capital formation and risk management. While privacy-preserving technologies are important, commercial integrity also requires enough transparency for participants to assess counterparty trustworthiness and for regulators to maintain oversight. This pillar balances privacy protection with the transparency essential for commercial integrity, supporting research showing that properly structured decentralized exchanges can match the market quality of centralized venues (Barbon & Ranaldo, 2024).

Pillar 3: On-Chain Segregation of Duties

What it means: Key roles within the ecosystem—protocol builders, auditors, compliance developers, application builders, and governance participants—must maintain demonstrable independence, with regulatory oversight maintaining appropriate separation from commercial interests. This independence can be verified through a combination of off-chain attestations and on-chain identity mechanisms. Iterative ownership mapping ensures that complex token structures do not obscure concentrated control across supposedly independent functions (Nadler & Schär, 2021). This helps ensure that no single entity exercises undue influence across multiple critical functions.

Why it's crucial: This prevents conflicts of interest that have historically undermined financial system integrity, such as when the same entities provide both custody and trading services (enabling front-running), when protocol developers control supposedly independent governance processes, or when compliance verification is controlled by the same parties who benefit from approval. Built-in checks and balances create systemic resilience and support the fairness, accountability, and legitimacy essential for institutional participation. Contrast this with successful segregation: the recent TWAMM hook development exemplified proper separation (Adams et al., 2021)—Paradigm provided research, FWB DAO governed deployment decisions, Uniswap Labs supplied infrastructure, Zaha Studio handled implementation, and external

auditors verified security. This collaborative model with clear role boundaries enabled sophisticated institutional treasury management capabilities while maintaining system integrity.

Pillar 4: Modular and Scoped Stakeholder Governance

What it means: Governance isn't a one-size-fits-all monolith. It should be granularly scoped, allowing stakeholders directly impacted by a specific smart contract, liquidity pool, or commercial activity to have proportionate say over its specific rules and parameters. Tiered structures can allow for different levels of influence based on stake, expertise, or role. For example, liquidity providers in a specific stablecoin pool would have governance rights over that pool's fee structures and risk parameters, while having no vote on unrelated pools' operations. Research on DeFi lending protocols demonstrates how properly scoped governance can improve interest rate efficiency and liquidity provision while maintaining market integrity (Zhang et al., 2023).

Why it's crucial: This ensures that decisions are made by those with the most relevant context and vested interest, leading to more efficient, fair, and responsive governance. It avoids situations where unrelated parties dictate terms for specific market segments, and instead promotes order, accountability, scalability, and legitimacy. Scoped governance also enhances regulatory oversight by making governance decisions transparent and traceable, creating clear accountability chains that can be customized for different jurisdictions.

Research on DeFi governance patterns reveals the importance of proper stakeholder scoping, with systematic reviews showing that governance structures significantly impact protocol sustainability and user protection (Siriwardana et al., 2023). Analysis of "vampire attacks" shows that governance captured by short-term incentive seekers rather than stakeholders with genuine long-term interests in specific market segments tends to fail over time, as evidenced by the long-term performance gaps between projects that relied on token rewards versus those that built sustainable community engagement.

Pillar 5: Adaptable Governance without Market Disruption

What it means: Web3 systems are not static. The ability to upgrade contracts, modify rules, or respond to new threats is vital. However, this adaptability must be managed through governance processes that allow changes to be implemented smoothly, without halting markets, losing user funds, or breaking dependent applications. Mechanisms like timelocks, proxy contracts, and phased rollouts are key. This includes responding to evolving regulatory requirements, security discoveries, and market conditions while maintaining operational continuity.

Why it's crucial: This ensures long-term viability and trustworthiness in a rapidly evolving regulatory and technological landscape. Markets need to adapt to new compliance requirements, security threats, and operational improvements, but evolution should not come at the cost of stability and investor confidence. Systems that cannot adapt smoothly become

obsolete or face regulatory shutdown, while those that disrupt markets during updates damage user trust. This underpins orderly markets and sustained investor protection by enabling proactive rather than reactive responses to challenges.

The pressure for rapid deployment often conflicts with adaptability. The app-first blockchain strategy—where successful applications drive infrastructure choices—creates path dependencies. As user bases and institutional integrations grow, early architectural decisions become harder to change. This underscores the need to build adaptability from the start, rather than retrofitting it later.

These five conditions are interdependent requirements for achieving genuine commercial integrity in Web3 systems. Without them, systems inevitably rely on off-chain enforcement, centralized control points, or architectural compromises that undermine the transparency, fairness, and reliability essential for sustainable institutional adoption and regulatory compliance. Together, they provide a systematic foundation for building Web3 infrastructure that delivers on both technological innovation and commercial integrity outcomes.

4. The Imperative for Systematic Assessment

The absence of systematic commercial integrity assessment frameworks leads to fundamental market failure: stakeholders lack principled ways to distinguish genuine infrastructure innovation from sophisticated regulatory arbitrage. Current evaluation approaches rely on ad-hoc metrics—total value locked, user counts, technical audits—that fail to capture the architectural foundations necessary for sustainable commercial integrity. This analytical gap becomes increasingly costly as major infrastructure decisions compound daily, demanding systematic evaluation frameworks that can assess commercial integrity architecture rather than surface-level indicators.

Implementing systematic commercial integrity assessment requires concrete measurement methodologies, particularly for governance evaluation. Recent empirical research on DeFi token distribution reveals that governance concentration problems are already widespread, with some protocols showing extreme ownership concentration despite sophisticated technical architectures (Nadler & Schär, 2021). Systematic assessment must therefore include iterative ownership mapping to identify true beneficial control across complex token structures, as governance concentration directly undermines Pillars 2, 3, and 4 regardless of surface-level technical sophistication.

Architectural Assessment Beyond Technical Metrics

The five-pillar framework transforms evaluation methodology by focusing on foundational capabilities rather than operational outcomes. Traditional assessment approaches examine whether systems currently work—measuring transaction volumes, security incidents, or user satisfaction. Systematic commercial integrity assessment instead evaluates whether systems

can sustain commercial integrity under stress—such as regulatory changes, market volatility, governance disputes, or security threats. Recent analysis demonstrates that blockchain technology can achieve atomic settlement, where "asset transfers occur simultaneously and irrevocably, or not at all." This provides the technical foundation for atomic rule enforcement across all compliance requirements (ElBendary, 2025; Le & Campbell, 2025).

Consider cross-chain liquidity protocols. Conventional assessment focuses on successful transaction volumes and total value locked. Systematic assessment using the five pillars reveals critical architectural questions: Does atomic enforcement extend beyond technical atomicity to include regulatory compliance verification? Can trust assessment mechanisms distinguish between genuine commercial activity and artificially generated metrics? Are governance structures properly segregated to prevent conflicts of interest between protocol development, auditing, and regulatory compliance functions?

This analytical depth exposes the difference between systems that currently function and systems architecturally capable of sustained commercial integrity. The framework's evaluative power lies not in identifying immediate operational problems, but in revealing architectural limitations that will create systematic failures as adoption scales or regulatory requirements evolve.

Pattern Recognition Across Infrastructure Types

Systematic assessment enables pattern recognition across otherwise disparate Web3 implementations. Government crypto initiatives, enterprise blockchains, DeFi protocols, and NFT marketplaces all share fundamental commercial integrity requirements, despite technical differences. The five-pillar framework offers consistent analytical criteria to reveal common failure modes across these diverse applications.

Infrastructure patterns emerge through systematic evaluation. Systems that promise compliance through technical innovation alone often exhibit weak governance segregation and limited regulatory adaptability. Platforms with impressive user metrics frequently rely on engagement patterns inconsistent with genuine commercial participation. High-performance technical architectures may force users to manually verify critical security contexts rather than enforcing verification atomically.

These patterns become visible only through systematic architectural assessment. Ad-hoc evaluation approaches miss these fundamental similarities because they focus on application-specific metrics rather than underlying commercial integrity capabilities. The framework's analytical consistency enables stakeholders to apply lessons learned from one infrastructure type to evaluate seemingly unrelated systems.

The framework's evaluative power extends beyond assessment to informing better architectural design. Recent systematic approaches to Web3 infrastructure, such as the Hook Manager

Framework for Uniswap v4 (ElBendary, 2025), demonstrate how the five-pillar requirements can be embedded into protocol design through modular policy enforcement and decentralized governance. Such frameworks provide practical validation that commercial integrity requirements are achievable through systematic architectural patterns rather than ad-hoc solutions.

Institutional Due Diligence Framework

Institutional adoption demands evaluation capabilities that extend far beyond current assessment methodologies. When pension funds, sovereign wealth entities, or multinational corporations evaluate Web3 infrastructure, they require comprehensive frameworks addressing governance accountability, regulatory adaptability, operational resilience, and long-term commercial viability. Traditional technical due diligence cannot answer these institutional requirements.

The five-pillar structure provides systematic institutional assessment methodology. Rather than subjective risk evaluation, institutions can systematically assess whether specific infrastructure exhibits the architectural capabilities necessary for sustained commercial integrity. Does the system enforce compliance rules atomically across all transaction contexts? Can stakeholders assess counterparty trustworthiness through verifiable on-chain mechanisms? Are governance structures appropriately segregated and scoped to prevent conflicts of interest?

This systematic approach transforms institutional evaluation from intuitive risk assessment to analytical architectural review. Institutions can evaluate infrastructure against consistent criteria, compare competing platforms using shared standards, and identify specific architectural improvements necessary for institutional adoption. The framework enables institutional stakeholders to move beyond vague notions of "blockchain risk" toward precise assessment of commercial integrity.

Regulatory Assessment Methodology

Regulators face parallel analytical challenges when evaluating Web3 infrastructure for compliance potential. Traditional regulatory frameworks focus on outcomes—whether systems currently protect investors, maintain market integrity, or facilitate capital formation. Systematic commercial integrity assessment evaluates architectural capacity—whether systems can deliver these outcomes consistently across evolving regulatory requirements.

The normative theory provides regulators with architectural assessment criteria rather than application-specific compliance checklists. Instead of evaluating individual protocols case by case, regulators can assess infrastructure capabilities against the five pillars to determine compliance potential—shifting regulatory evaluation from reactive enforcement to proactive architectural analysis.

Systematic assessment enables more sophisticated regulatory approaches. Rather than binary approval or prohibition decisions, regulators can identify specific architectural improvements that would enable compliance, develop tiered oversight approaches based on commercial integrity capabilities, and distinguish between systems requiring extensive supervision and those architecturally capable of self-enforcement.

Market Efficiency Through Systematic Assessment

Current market inefficiencies stem directly from inadequate assessment frameworks. Capital and users flow toward systems with sophisticated marketing rather than robust commercial integrity architecture, creating misallocation that slows ecosystem maturation. Projects with weak foundational capabilities but effective promotion can attract resources away from architecturally superior but less visible alternatives.

Systematic commercial integrity assessment addresses these market failures by providing consistent evaluation criteria that reveal architectural capabilities independent of promotional effectiveness. The framework enables efficient capital allocation based on foundational commercial integrity rather than surface-level appeal.

Moreover, systematic assessment frameworks create positive selection pressure. As institutional stakeholders and sophisticated users adopt consistent evaluation criteria, projects are incentivized to improve commercial integrity architecture rather than simply optimize for promotion. This evolutionary pressure accelerates the ecosystem's maturation toward truly sustainable commercial infrastructure.

The imperative for systematic assessment transcends individual infrastructure evaluation—it addresses fundamental analytical gaps that currently prevent efficient market operation, institutional adoption, and regulatory clarity. As Web3 infrastructure choices compound daily with potentially irreversible consequences, implementing systematic commercial integrity assessment frameworks becomes essential for ecosystem sustainability and long-term commercial viability.

5. Implications and the Path Forward

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.

5.1. The Cost of Delayed Action

Current market conditions provide compelling evidence for this theory's urgency. User experience problems persist across DeFi—with users forced to manually manage complex token approval matrices, 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—creating 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—exactly the kind of systematic vulnerability that atomic on-chain rule enforcement and proper trust assessment mechanisms would prevent. These failures create additional uncertainty costs beyond regulatory concerns, showing how architectural gaps undermine investor protection even in technically advanced platforms.

Historical precedent demonstrates how infrastructure compromises compound. 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 'by the time information technology made a direct, decentralized system wholly realizable, the option was more or less excluded by the SEC and major market participants.' Today's Web3 infrastructure decisions face identical dynamics—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—exactly the kind of systematic integrity failure that proper on-chain trust assessment and atomic rule enforcement would prevent, showing how current architectural gaps create multiple pathways to commercial integrity breakdown.

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).

5.2. The Path Forward

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

Kazakhstan announces "CryptoCity" where cryptocurrency will be used for "purchasing goods, services, and even beyond" (Zmudzinski, 2025)—a comprehensive crypto economy requiring robust commercial integrity but being planned without apparent systematic architecture 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: institutional RWA integration proceeds using infrastructure that cannot deliver promised compliance capabilities, stablecoin networks launch without addressing fundamental monetary integration challenges, and new L1s prioritize 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.

6. 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 provides both the architectural principles necessary for building robust commercial infrastructure and the systematic assessment framework required to evaluate existing systems. The five pillars—atomic enforcement, on-chain trust assessment, segregated duties, scoped governance, and adaptable systems—offer stakeholders consistent criteria for distinguishing between genuine innovations and sophisticated regulatory arbitrage.

The evidence is clear: current ad-hoc approaches create systematic market failures, institutional uncertainty, and architectural risks that compound as adoption scales. Projects with billions in TVL suffer security failures that proper architectural frameworks would prevent. Governments' crypto initiatives launch without commercial integrity foundations. Capital misallocates toward marketing sophistication rather than architectural quality.

The imperative is immediate. Each day brings infrastructure decisions that become exponentially more expensive to correct as user bases and institutional integrations lock in architectural choices. The opportunity exists now to build Web3 commerce on integrity by design rather than retrofit solutions onto problematic foundations.

This theory provides the framework. Implementation requires coordinated adoption by builders committed to sustainable architecture, institutions demanding systematic assessment criteria, and regulators embracing technology-native approaches to commercial integrity. The choice is

ours: architect the future of commerce on integrity, or fragment Web3's transformative potential through compromises that serve no one's long-term interests.

The window for systematic action is still open—but it is closing rapidly.

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., & Ranaldo, 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.

ElBendary, 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-cryptocity-crypto-payments-adoption