Use-Case-Driven Blockchain Architectures in Financial Enterprises: Permissioned, Consortium, Hybrid, and Public Networks

Ian Staley
Independent Researcher, USA

* Corresponding author. Email: ian.t.staley@gmail.com (I.S.)
Manuscript received February 1, 2026; accepted February 28, 2026; published March 19, 2026.
DOI: 10.18178/IJBTA. 2026.4.1.20-33

Abstract: Financial enterprises increasingly face architectural decisions regarding the use of permissioned, consortium, public, or hybrid blockchain networks as digital assets, tokenized instruments, and distributed ledger technologies move from experimentation to production deployment. Much of the existing discourse frames blockchain adoption as a binary choice between private and public networks, overlooking the reality that financial use cases exhibit materially different requirements across privacy, governance, compliance, scalability, interoperability, and market access. This paper advances a use-case-driven architectural framework for blockchain adoption in financial enterprises, arguing that architecture selection should be determined by functional and regulatory requirements rather than ideological preferences for decentralization. Drawing on academic literature, industry research, and emerging regulatory guidance, the study comparatively examines permissioned, consortium, and public blockchain architectures within the context of core financial use cases, including enterprise resource planning integration, primary asset issuance, secondary market trading, and settlement. The analysis highlights how permissioned and consortium networks provide strong governance, confidentiality, and compliance alignment for internal operations and regulated issuance, while public blockchains offer liquidity, composability, and interoperability advantages for secondary markets and open settlement. The paper proposes a hybrid architectural reference model in which multiple blockchain network types coexist across the asset lifecycle, interconnected through interoperability layers and compliance-aware integration mechanisms. This approach reflects the evolving structure of financial market infrastructure and provides a practical foundation for scalable, compliant, and future-ready blockchain deployment in financial enterprises.

Keywords: blockchain architecture, financial enterprises, Tokenization, hybrid blockchain, distributed ledger technology

1. Introduction

Blockchain technologies have transitioned from experimental infrastructures to increasingly material components of financial market modernization. As financial institutions explore Distributed Ledger Technologies (DLT) for asset tokenization, payments, settlement, and internal Operational Efficiencies, architectural decisions regarding network design have become central to both technical viability and regulatory alignment. Rather than a monolithic technological choice, blockchain adoption in financial enterprises now represents a portfolio of architectural decisions shaped by distinct functional, institutional, and compliance-driven requirements.

Prevailing discourse in both academic and industry literature often frames blockchain adoption as a dichotomy between permissioned and public networks. While this framing offers conceptual simplicity, it obscures the heterogeneous nature of financial use cases and the differentiated constraints under which financial institutions operate. Privacy obligations, governance requirements, settlement finality, interoperability needs, and regulatory compliance, particularly with respect to Anti–Money Laundering (AML), Counter-Terrorist Financing (CTF), and travel rule obligations, vary significantly across internal enterprise systems, primary market issuance, and secondary market trading environments [1–3]. As a result, no single blockchain architecture can optimally satisfy all enterprise financial requirements.

Financial enterprises increasingly confront this reality as tokenization initiatives mature beyond proof-of-concept deployments. Internal applications such as enterprise resource planning integration, reconciliation, and post-trade processing prioritize confidentiality, deterministic governance, and operational control, making permissioned architectures a natural fit [4–6]. In contrast, secondary markets for tokenized assets benefit from the liquidity, composability, and global accessibility characteristic of public blockchain networks, particularly where neutral settlement infrastructure and open participation are essential [7, 8]. Between these extremes, consortium-based networks have emerged as a mechanism for regulated primary issuance and trusted participant ecosystems, balancing shared governance with controlled access [9–11].

Recent developments in public blockchain scalability and infrastructure further complicate architectural decision-making. Advances in layer-two rollups, data availability mechanisms, and blob-based storage on Ethereum reflect an evolving technical landscape in which performance, cost, and decentralization trade-offs continue to shift [12–14]. At the same time, interoperability frameworks such as Cosmos Inter-Blockchain Communication (IBC), cross-chain messaging protocols, and application-specific chains have expanded the feasibility of multi-network architectures spanning heterogeneous blockchain environments [15–18]. These developments reduce the need for architectural exclusivity and instead enable composable, layered designs.

Against this backdrop, financial institutions are increasingly converging on hybrid blockchain architectures that align network types with specific phases of the asset and transaction lifecycle. Permissioned and consortium networks support origination, issuance, and internal processing, while public networks provide settlement finality, liquidity access, and cross-ecosystem interoperability. Such architectures reflect not ideological compromise but pragmatic engineering, consistent with regulatory expectations and the evolving structure of financial market infrastructure articulated by global standard-setting bodies [19, 20]. This paper advances a use-case-driven framework for evaluating blockchain architectures in financial enterprises, emphasizing alignment between functional requirements and network design as the foundation for scalable and compliant adoption.

2. Literature Review and Theoretical Foundation

Academic literature on blockchain adoption has evolved from early explorations of cryptographic trust and decentralized consensus toward more nuanced analyses of architectural design, governance, and enterprise integration. Recent surveys emphasize that blockchain systems should be understood not as a singular technology but as a spectrum of architectural patterns, including private, consortium, public, and hybrid configurations, each optimized for different operational contexts [21–24]. This shift reflects growing recognition that performance, governance, and compliance constraints materially influence system design choices, particularly in regulated industries such as financial services.

Architectural pattern research has increasingly focused on how blockchain systems are composed and integrated within broader enterprise environments. Studies examining monolithic versus microservices-based blockchain architectures highlight the importance of modularity, scalability, and operational resilience

when deploying DLT alongside legacy financial systems [4, 25]. Permissioned blockchain platforms have been shown to offer advantages in throughput, deterministic governance, and auditability, making them suitable for internal financial processes and regulated workflows [5, 6]. At the same time, comparative analyses demonstrate that these benefits often come at the expense of open participation and cross-network composability.

Parallel literature on tokenization and digital asset infrastructure underscores the growing role of blockchain networks as financial market infrastructure rather than standalone applications. Industry and academic research describe tokenization as a mechanism for modernizing asset issuance, distribution, and settlement by embedding financial instruments directly into programmable networks [7, 9, 26]. Within this context, consortium-based architectures have emerged as a pragmatic middle ground, enabling shared governance among trusted participants while maintaining controlled access and regulatory oversight [10, 21]. Governance-focused scholarship further examines whether permissionless public systems can satisfy securities market requirements, generally concluding that unrestricted participation remains misaligned with many primary market obligations [27].

Public blockchain literature has concentrated on scalability, interoperability, and network effects. Advances in layer-two rollups, sharding strategies, and data availability mechanisms have significantly altered the performance characteristics of public networks, reduced transaction costs and improving throughput without fully sacrificing decentralization [12−14]. Concurrently, interoperability research highlights the growing feasibility of cross-chain communication through standardized messaging protocols and application-specific chains, enabling assets and state to move across heterogeneous blockchain environments [15−18]. These developments challenge earlier assumptions that enterprises must select a single blockchain network for all use cases.

Regulatory and compliance-oriented scholarship provides an additional theoretical foundation for architectural differentiation. Frameworks addressing blockchain compliance emphasize that AML, CTF, travel rule, and stablecoin regulations impose architectural constraints that vary across transaction types and market structures [1−3, 26]. Global policy institutions increasingly describe future financial systems as hybrid in nature, combining private control mechanisms with public settlement infrastructure to balance innovation, stability, and regulatory effectiveness [19, 20]. Taken together, the literature supports a use-case-driven perspective in which blockchain architectures are selected and combined based on functional requirements, regulatory obligations, and market structure rather than technological ideology. From an architectural perspective, Table 1 functions as a design decision aid, translating non-functional and functional requirements into network selection guidance across the financial asset lifecycle.

Additional surveys and system-level studies further contextualize enterprise blockchain adoption within broader financial and infrastructural transformations. Research on wholesale central bank digital currencies and institutional settlement systems highlights how permissioned and consortium-led infrastructures are often favored for systemic stability and monetary control [28−30]. Large-scale surveys of distributed ledger technologies reinforce the importance of scalability, governance, and integration when deploying blockchain systems in regulated environments [31, 32]. Related work examining unified blockchain data structures and secure appchain architectures underscores the growing emphasis on modularity, interoperability, and system-level abstraction as blockchain ecosystems mature [33, 34].

Table 1. Financial Use Cases, Key Requirements, and Preferred Blockchain Architectures

Financial Use Case	Key Requirements	Preferred Architecture	Rationale
Internal ERP, accounting, and reconciliation	High confidentiality, deterministic governance, auditability, low latency	Permissioned	Enterprise financial operations prioritize privacy, control, and integration with legacy systems, which permissioned DLT platforms are designed to support [4–6].
Interbank processes and shared infrastructure	Controlled access, shared governance, regulatory alignment	Consortium	Consortium networks enable collaboration among trusted institutions while maintaining governance structures compatible with regulatory oversight [10, 11, 27].
Primary issuance of tokenized assets	Participant vetting, compliance enforcement, issuance controls	Consortium / Permissioned	Regulated issuance requires whitelisted participation and compliance controls that are difficult to enforce in open public networks [9, 11, 26].
Secondary market trading of tokenized assets	Liquidity, composability, global accessibility	Public	Public blockchains provide network effects and composability essential for liquidity formation and open market participation [7, 8].
Settlement and cross-asset interoperability	Neutral infrastructure, finality, cross-network connectivity	Public / Hybrid	Public networks increasingly serve as neutral settlement layers, while hybrid models mitigate compliance and governance constraints [12, 15, 19].
End-to-end asset lifecycle management	Segmented controls, interoperability, regulatory compliance	Hybrid	Hybrid architectures align different network types with specific lifecycle phases, optimizing both control and market access [23, 24, 31].

3. Research Methodology

This research adopts a qualitative, architecture-centered methodology designed to evaluate blockchain network models in the context of financial enterprise use cases. Rather than empirical testing or protocol-level benchmarking, the study focuses on comparative architectural analysis to assess how different blockchain configurations align with functional, operational, and regulatory requirements in financial systems. This approach is appropriate given the heterogeneous nature of blockchain deployments and the early stage of many large-scale institutional implementations.

The analytical framework integrates three complementary methods. First, a structured literature review synthesizes academic research on blockchain architectures, enterprise DLT design patterns, and tokenized financial infrastructure. This review establishes a theoretical foundation for understanding architectural trade-offs across permissioned, consortium, public, and hybrid networks [21–23]. Second, use-case requirement mapping is employed to identify the specific constraints and objectives associated with distinct financial activities, including internal enterprise operations, asset issuance, secondary market trading, and settlement. These requirements are then systematically mapped to architectural characteristics such as governance models, privacy mechanisms, scalability approaches, and interoperability capabilities.

In addition, comparative architectural reasoning is applied to evaluate how emerging infrastructure developments, such as layer-two scalability mechanisms, data availability innovations, and cross-chain interoperability frameworks, affect the suitability of different network types for financial enterprise deployment [12, 13, 15]. Regulatory considerations are incorporated as architectural constraints rather than external variables, reflecting the reality that compliance obligations shape network design choices in financial institutions [1, 2, 28]. The methodology emphasizes design generalizability over case-specific optimization, enabling the development of a reference architecture applicable across multiple financial contexts. By grounding architectural evaluation in established literature and clearly defined use-case requirements, the study provides a practical framework for financial enterprises assessing blockchain adoption strategies under evolving technical and regulatory conditions.

4. Use-Case Requirements in Financial Enterprises

Financial enterprises operate across a diverse set of functional domains, each characterized by distinct

operational objectives and regulatory constraints. Unlike consumer-facing or experimental blockchain applications, enterprise financial use cases are shaped by strict requirements related to confidentiality, governance, auditability, compliance, and system interoperability. These requirements vary materially depending on whether blockchain technology is applied to internal operations, regulated market infrastructure, or open financial ecosystems, making architectural differentiation a necessity rather than an optimization choice. These use cases can be understood as distinct stages of the financial asset lifecycle, from internal origination and accounting, through regulated issuance, to open market trading and settlement, each imposing different architectural constraint.

Internal financial systems represent one of the earliest and most mature domains for blockchain adoption. Functions such as enterprise resource planning integration, reconciliation, internal settlements, and audit support prioritize data confidentiality, deterministic transaction finality, and tightly controlled governance structures. In these contexts, participants are known entities operating within established legal frameworks, and system performance is often more critical than open accessibility. These requirements also intersect with broader data architecture considerations, as financial institutions increasingly integrate blockchain platforms with large-scale analytics, reporting, and risk management systems that rely on heterogeneous data pipelines [17]. Permissioned blockchain architectures align well with these requirements by enabling fine-grained access controls, predictable governance processes, and integration with existing enterprise technology stacks [4–6].

Primary market activities introduce additional complexity by extending participation beyond a single organization while remaining subject to regulatory oversight. The issuance of tokenized assets, including deposits, funds, and other regulated financial instruments, requires participant vetting, compliance enforcement, and shared governance among trusted institutions. Consortium-based architectures have emerged as a practical solution in this domain, allowing multiple financial entities to coordinate issuance and lifecycle management while maintaining control over network membership and rule enforcement [9–11]. Such architectures support regulatory expectations for transparency and accountability while avoiding the unrestricted access characteristic of public networks.

Secondary market trading environments impose a different set of requirements centered on liquidity, price discovery, and interoperability. Open participation, composability with decentralized applications, and access to global pools of capital are critical drivers of market efficiency in these contexts. Public blockchain networks are uniquely positioned to satisfy these requirements due to their neutral infrastructure, standardized interfaces, and network effects that support liquidity formation across asset classes [7, 8]. While these networks introduce challenges related to governance and compliance, they provide capabilities that are difficult to replicate within closed or permissioned systems.

Settlement and cross-asset interoperability further complicate architectural considerations. In this context, settlement refers to the irrevocable transfer of value and legal finality, rather than pre-trade matching or clearing functions, which often remain within existing market infrastructure. Financial institutions increasingly require neutral settlement layers capable of interfacing with multiple asset types, platforms, and jurisdictions. Recent advances in public blockchain scalability, including layer-two execution environments and data availability optimizations, have strengthened the viability of public networks as settlement infrastructure without fully compromising decentralization [12–14]. At the same time, interoperability frameworks such as inter-chain communication protocols and cross-chain messaging systems enable assets and state to move between heterogeneous networks, reducing the need for architectural exclusivity [15, 16, 18, 20].

Regulatory compliance requirements cut across all financial use cases and function as architectural constraints rather than external considerations. Obligations related to AML, CTF, travel rule compliance, and

stablecoin regulation influence network design decisions by shaping access controls, data availability, and governance mechanisms [1–3, 28]. Global policy perspectives increasingly recognize that future financial infrastructure will consist of hybrid arrangements combining private control environments with public settlement and interoperability layers [19, 20]. These requirements collectively support the conclusion that financial enterprises benefit from architectures that align specific network types with distinct functional roles across the asset and transaction lifecycle.

Table 2 consolidates these requirements into a comparative decision matrix, illustrating how specific financial use cases map to preferred blockchain architectures based on functional and non-functional constraints. Rather than prescribing a single architectural model, the table highlights how variations in confidentiality, governance, compliance enforcement, and market access directly influence network selection. This mapping reinforces the central argument of the paper: blockchain architecture in financial enterprises is best understood as a use-case-driven design decision, not a uniform platform choice.

Table 2. Architectural Trade-Off Comparison Across Blockchain Network Types

Architecture Type	Governance Model	Privacy & Access Control	Performance & Scalability	Interoperability	Regulatory Alignment	Typical Financial Applications
Permissioned	Centralized or federated governance among known entities	Strong privacy through identity-based access controls	High throughput and low latency due to controlled participation	Limited by design; typically requires adapters or gateways	High alignment with AML, CTF, and audit requirements	Internal ERP integration, reconciliation, internal settlement, audit trails
Consortium	Shared governance among vetted participants	Controlled access with shared compliance rules	Moderate to high performance depending on consensus design	Moderate; supports inter-organizational workflows	Strong alignment for regulated issuance and interbank use cases	Primary issuance of tokenized assets, interbank processes, shared infrastructure
Public	Decentralized governance with open participation	Limited native privacy; relies on cryptographic techniques and overlays	Improving scalability through layer-two solutions and data availability mechanisms	High; composability and open standards enable cross-application integration	Variable; requires additional compliance layers	Secondary market trading, open settlement, liquidity provisioning
Hybrid	Layered governance across multiple network types	Segmented privacy models aligned to functional domains	Optimized by assigning workloads to appropriate layers	High; designed explicitly for cross-network coordination	High when compliance is enforced at controlled layers	End-to-end asset lifecycle management, institutional tokenization, cross-market settlement

Notes: This comparison reflects architectural characteristics synthesized from enterprise blockchain design literature and financial market infrastructure research [5, 6, 15, 19, 21, 23].

5. Architectural Models: Permissioned, Consortium, and Public Networks

Permissioned blockchain architectures are most commonly adopted in financial enterprises where participants are known, roles are well defined, and operational control is a primary concern. These networks typically employ identity-based access controls, deterministic governance mechanisms, and consensus models optimized for performance rather than open participation. As a result, permissioned systems can achieve high throughput, low latency, and predictable finality, making them suitable for internal financial operations such as accounting, reconciliation, and audit support [4–6]. Their closed nature also

simplifies compliance with regulatory requirements related to data privacy, auditability, and operational risk management. Systematic comparisons of permissioned and hybrid ledger implementations further indicate that architectural choices are strongly influenced by performance isolation, security boundaries, and operational governance rather than protocol-level decentralization alone [25].

Beyond single-institution deployments, consortium blockchain architectures extend permissioned principles to multi-entity environments. In consortium networks, governance authority is distributed among a defined set of trusted participants, such as banks, asset managers, or market infrastructure providers. This shared governance model enables coordination across organizations while preserving access controls and compliance enforcement [10, 11, 27]. Consortium architectures are particularly well suited to regulated primary market activities, including the issuance and lifecycle management of tokenized assets, where participant vetting and rule enforcement are essential. However, increased governance complexity and coordination overhead can limit scalability and slow decision-making compared to fully centralized permissioned systems.

Public blockchain networks represent a fundamentally different architectural model characterized by open participation, decentralized governance, and global accessibility. These networks excel in environments where liquidity, composability, and neutral infrastructure are critical, such as secondary market trading and open settlement layers for tokenized assets [7, 8]. Recent advances in scalability, including layer-two execution environments, sharding strategies, and data availability mechanisms, have improved the performance characteristics of public networks, making them increasingly viable for financial use cases that were previously impractical at scale [12−14]. Despite these improvements, public networks introduce challenges related to governance coordination, privacy, and regulatory compliance, often necessitating additional architectural layers to meet institutional requirements.

Taken together, the literature suggests that permissioned, consortium, and public blockchain architectures should be viewed as complementary rather than mutually exclusive. Each model exhibits strengths aligned to specific functional domains within financial enterprises, as well as limitations that become pronounced when applied outside those domains. This recognition has driven growing interest in hybrid architectures that combine multiple network types across the financial asset lifecycle, enabling enterprises to balance control, compliance, and market access through layered architectural design.

6. Hybrid Blockchain Architectures for Financial Enterprises

Hybrid blockchain architectures have emerged as a pragmatic response to the structural diversity of financial enterprise requirements. Hybrid architectures are defined here not by technical integration alone, but by deliberate allocation of trust, control, compliance, and openness across distinct network layers. Rather than attempting to force all financial activities onto a single network type, hybrid models allocate distinct functional roles to permissioned, consortium, and public blockchains across the asset and transaction lifecycle. This approach reflects an architectural recognition that control, compliance, and market openness are not uniformly required at every stage of financial operations, and that aligning network characteristics to specific use cases produces more resilient and scalable systems [23, 24]. Such hybrid architectures align with emerging institutional deployment patterns observed among global asset managers, banks, and market infrastructure providers pursuing tokenized funds, deposits, and settlement networks under regulated conditions [7, 10, 11].

In practice, hybrid architectures typically anchor internal enterprise processes within permissioned environments. Core financial functions such as enterprise resource planning integration, internal accounting, reconciliation, and risk reporting benefit from deterministic governance, identity-based access control, and low-latency execution [4−6]. These systems operate within well-defined trust boundaries and

legal jurisdictions, enabling financial institutions to meet audit, data residency, and operational risk requirements without exposing sensitive information to open networks. As a result, permissioned layers often serve as the system of record for internal financial state.

Moving outward from internal operations, consortium networks frequently support regulated inter-organizational workflows, particularly in primary market issuance and shared financial infrastructure. Tokenized deposits, funds, and other regulated instruments require participant vetting, rule enforcement, and coordinated governance across multiple institutions. Consortium architectures enable these capabilities by distributing control among trusted entities while preserving compliance mechanisms aligned with regulatory expectations [9−11]. This layer functions as a controlled interface between private enterprise systems and broader financial markets, reducing counterparty risk while enabling interoperability among participating institutions. Design considerations for deposit tokens and regulated payment instruments further support the use of controlled issuance environments, where governance, eligibility, and redemption logic can be enforced at the network layer [29, 30].

Public blockchain networks increasingly occupy the outer layers of hybrid financial architectures, particularly for secondary market trading, settlement, and liquidity access. Open participation, standardized interfaces, and composability make public networks well suited for price discovery and market efficiency [7, 8]. Advances in scalability, such as layer-two rollups, sharding techniques, and data availability innovations including blob-based storage, have materially improved the economic and performance characteristics of public networks, strengthening their viability as neutral settlement infrastructure [12−14]. These developments allow enterprises to leverage public networks without fully exposing internal systems to their governance or operational risks. Governance scholarship on distributed ledger systems applied to securities markets suggests that permissionless public governance models remain difficult to reconcile with regulatory accountability requirements, reinforcing the need for layered or hybrid governance structures [27].

Interoperability serves as the connective tissue of hybrid architectures, enabling coordination across heterogeneous blockchain environments. Cross-chain communication frameworks, inter-chain messaging protocols, and application-specific chains facilitate asset mobility and state synchronization between permissioned, consortium, and public networks [15, 16, 18, 20]. Rather than relying on monolithic bridges, modern hybrid designs increasingly emphasize modular interoperability layers that can enforce policy, validate state transitions, and preserve auditability across network boundaries. This approach reduces systemic risk while supporting composability across financial ecosystems.

Regulatory compliance considerations further reinforce the hybrid architectural paradigm. Obligations related to AML, CTF, travel rule enforcement, and stablecoin oversight impose differentiated requirements on transaction visibility, participant identification, and governance structures [1−3]. Studies examining stablecoins and real-world asset tokenization from a monetary and market-structure perspective further emphasize the role of architecture in balancing innovation with systemic risk and regulatory oversight [31]. Hybrid architectures allow compliance controls to be concentrated within permissioned and consortium layers, while public networks are leveraged for functions where transparency and openness are advantageous. Global policy institutions increasingly describe future financial systems as layered infrastructures that combine private control environments with public settlement and interoperability rails [19, 20]. Emerging protocol abstraction and context-management approaches have also been proposed as a means of coordinating state and execution logic across heterogeneous systems, reflecting broader trends toward modular and policy-aware interoperability [32]. Additional research further supports the view that hybrid architectures should be understood as part of a broader systems evolution in blockchain design rather than as isolated deployment choices. Recent work on deposit tokens and stablecoin-linked banking

responses highlights how regulated digital money instruments require carefully structured governance and redemption models in institutional settings [35, 36]. Emerging protocol and context orchestration research also suggests that modular coordination layers will become increasingly important as enterprises connect heterogeneous systems and execution environments [37]. Related studies on stablecoin design, on-chain treasury analytics, and digital-economy blockchain architectures reinforce the importance of composability, observability, and ecosystem-level integration in financial deployments [38–40]. Additional scholarship on blockchain use-case design, tokenized money frameworks, platform differentiation, and DLT adoption in financial systems further underscores that architectural selection depends not only on technical performance, but also on governance models, business process alignment, and institutional implementation constraints [41–45]. Policy and legal commentary on stablecoin implementation further illustrate how institutional architecture choices are shaped by emerging supervisory interpretations and implementation-specific rulemaking [46].

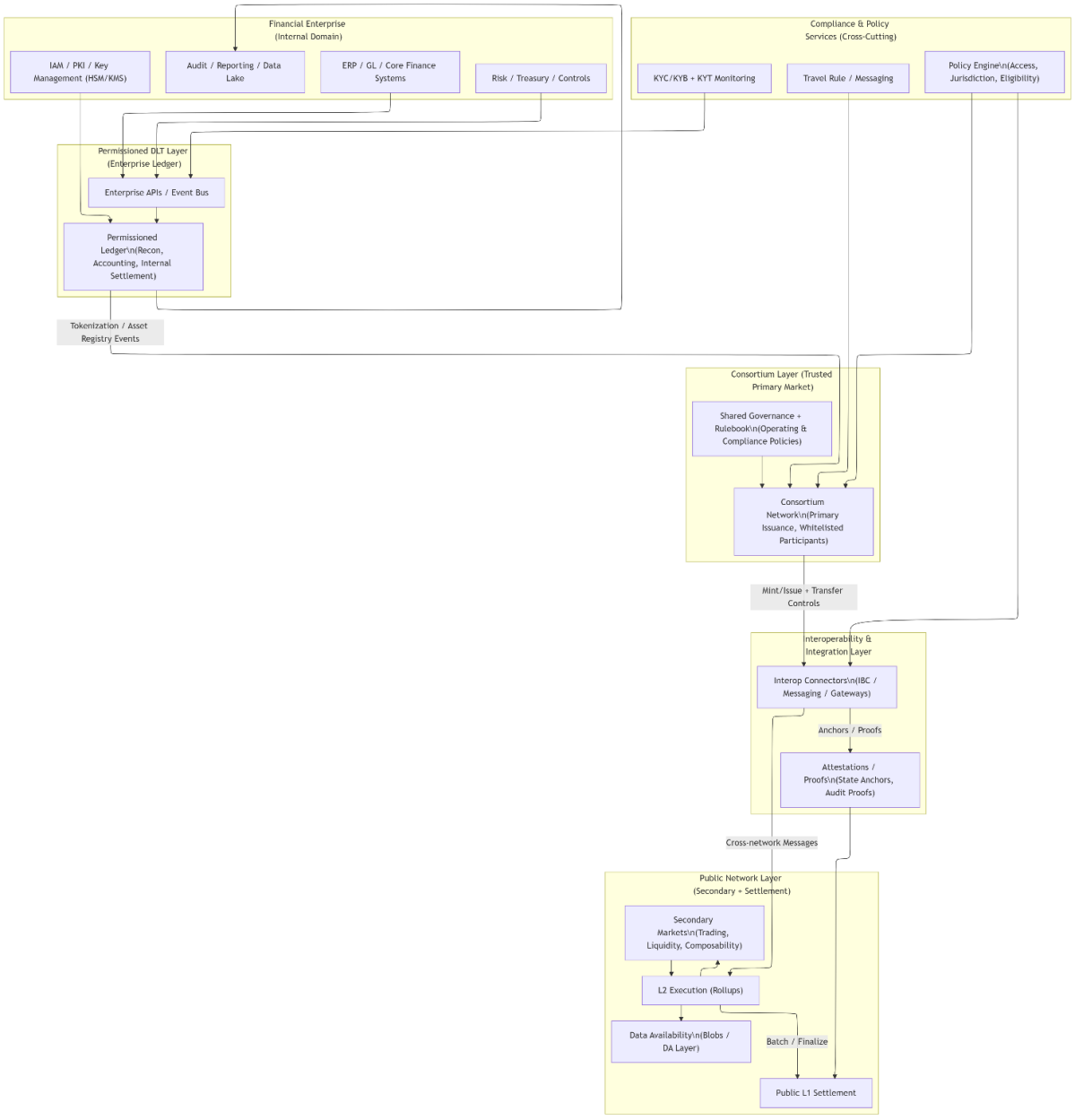

Fig. 1. Hybrid blockchain reference architecture for financial enterprises (permissioned + consortium + public settlement with interoperability and compliance layers).

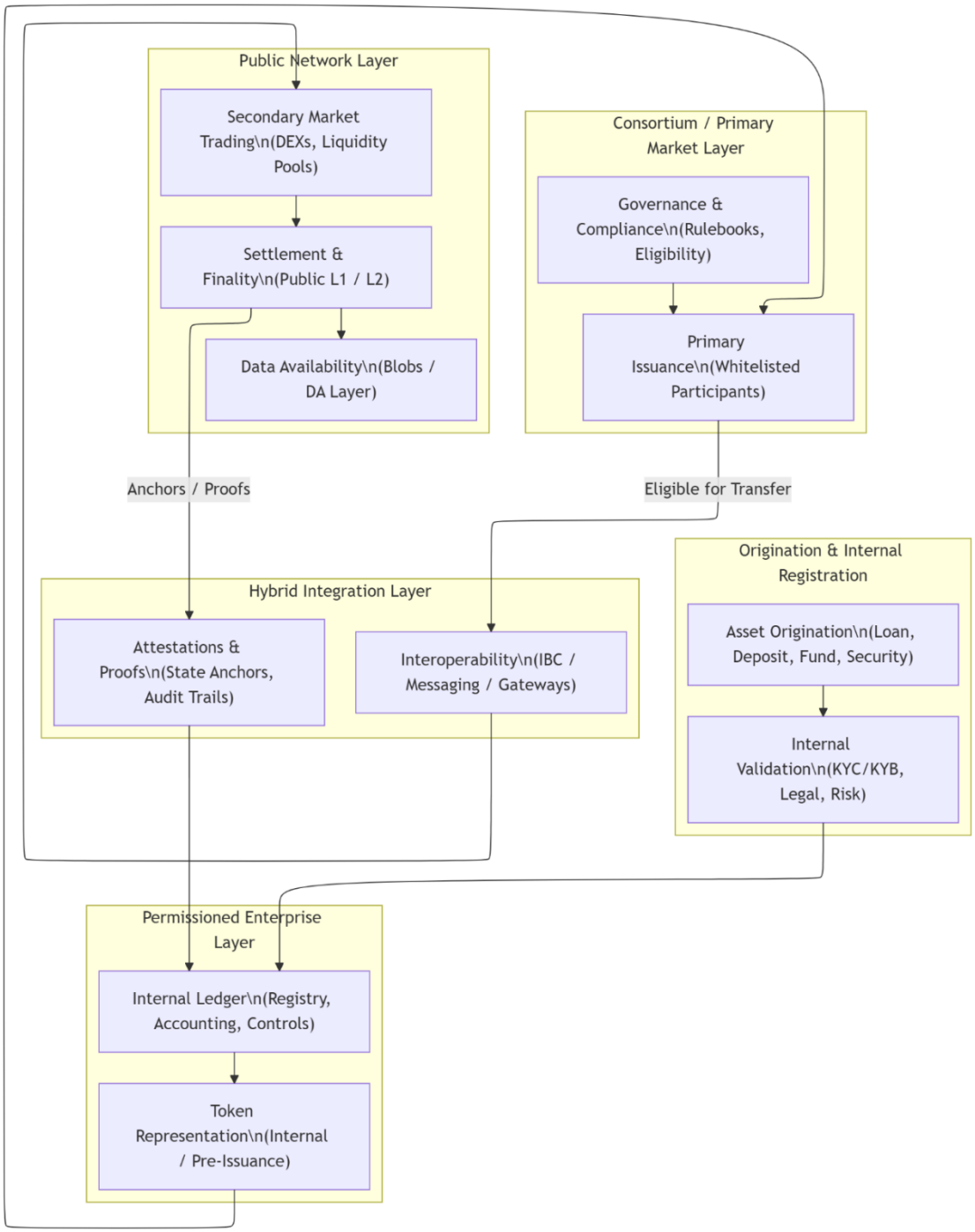

Fig. 2. Tokenized asset lifecycle across permissioned, consortium, hybrid, and public blockchain networks.

In sum, hybrid blockchain architectures represent a structural evolution of financial market infrastructure rather than a transitional compromise. In aligning network types with functional roles across the asset lifecycle, financial enterprises can balance operational control, regulatory compliance, and market efficiency within a single coherent design. The reference architecture presented in Fig. 1 and the lifecycle mapping illustrated in Fig. 2 formalize this approach, providing a framework for enterprises seeking to deploy blockchain technologies at scale under evolving technical and regulatory conditions.

Fig. 1 illustrates a layered hybrid blockchain architecture in which financial enterprise systems interface with multiple blockchain network types through explicit integration, compliance, and interoperability layers. Internal financial processes are anchored within a permissioned distributed ledger that serves as the

system of record for accounting, reconciliation, and risk management, while consortium networks support regulated primary issuance and inter-institutional coordination among trusted participants.

Public blockchain infrastructure is positioned as a settlement and liquidity layer, leveraging scalable execution environments and data availability mechanisms to support secondary market activity without exposing internal enterprise systems to open network governance. Interoperability components and attestation mechanisms connect these layers, enabling controlled asset movement, state verification, and auditability across heterogeneous networks while preserving compliance and operational boundaries.

Fig. 2 depicts the lifecycle of a tokenized financial asset as it progresses across distinct blockchain network types aligned with functional and regulatory requirements. Asset origination and validation occur within enterprise-controlled environments, where permissioned ledgers establish authoritative records for accounting, risk management, and compliance prior to market exposure.

Primary issuance is executed within consortium networks that enforce participant eligibility, governance rules, and regulatory controls, enabling coordinated distribution among trusted institutions. Once eligibility criteria are met, assets transition through interoperability and attestation layers into public blockchain environments, where secondary market trading, liquidity formation, and settlement finality occur. Ongoing anchoring and proof mechanisms enable state reconciliation and auditability across layers, reinforcing the role of hybrid architectures in supporting end-to-end asset lifecycle management without conflating control, compliance, and market access.

7. Limitations and Practical Challenges

Despite the architectural advantages of hybrid blockchain models, several limitations and practical challenges constrain their deployment in financial enterprises. One of the most significant challenges arises from regulatory fragmentation across jurisdictions, where differing interpretations of digital asset classification, stablecoin oversight, and compliance obligations complicate cross-border operations. While hybrid architectures can localize compliance controls within permissioned and consortium layers, coordinating regulatory alignment across interconnected networks remains a nontrivial operational burden [1−3, 28].

Operational complexity represents a second limitation inherent in multi-network designs. Hybrid architectures introduce additional layers for interoperability, policy enforcement, and state reconciliation, increasing system complexity relative to single-network deployments. This complexity can elevate implementation costs, lengthen deployment timelines, and expand the operational attack surface. Interoperability mechanisms, in particular, require careful governance and security design, as failures or misconfigurations at integration points may propagate risk across otherwise isolated networks [15, 16, 20].

Scalability and performance uncertainty further complicate long-term architectural planning. Although recent advances in layer-two execution environments, data availability mechanisms, and sharding strategies have materially improved public blockchain throughput and cost efficiency, these technologies remain subject to ongoing evolution [12−14]. Financial enterprises adopting hybrid architectures must therefore contend with the risk that performance assumptions made at design time may shift as public network economics and protocol parameters change over time.

Liquidity fragmentation presents an additional challenge for tokenized assets operating across multiple networks. While hybrid architectures allow enterprises to segment control and market access, asset liquidity may become dispersed across consortium and public environments, reducing market efficiency and complicating price discovery [8]. Managing liquidity migration between controlled issuance networks and open trading venues requires careful coordination to avoid market dislocation or unintended concentration risk.

Governance alignment across architectural layers also remains an open challenge. Permissioned and consortium networks typically rely on explicit governance structures, whereas public networks evolve through decentralized and often informal processes. Reconciling these governance models within a single operational framework can create tension, particularly when protocol upgrades, consensus changes, or policy modifications occur asynchronously across layers [23, 27]. Financial institutions must therefore design governance interfaces that anticipate and absorb such divergence. These limitations underscore that hybrid blockchain architectures are not a universal solution but rather a structured response to complex and evolving requirements. Addressing regulatory, operational, and governance challenges requires ongoing coordination among technical teams, compliance functions, and market participants. Recognizing these constraints is essential for realistic planning and for ensuring that hybrid architectures deliver sustainable value rather than short-term experimentation.

8. Conclusion

The evolution of blockchain adoption in financial enterprises reflects a broader shift from technology-centric experimentation toward architecture-driven infrastructure design. As digital assets, tokenized instruments, and distributed ledger technologies become embedded within core financial operations, the limitations of single-network approaches have become increasingly apparent. Financial use cases vary substantially in their requirements for governance, privacy, compliance, scalability, and market access, making architectural differentiation a foundational necessity rather than an implementation detail.

This paper has advanced a use-case-driven framework for evaluating blockchain architectures in financial enterprises, demonstrating how permissioned, consortium, and public networks each align with distinct functional domains. Permissioned architectures support internal enterprise operations where control, auditability, and deterministic governance are paramount. Consortium networks enable regulated coordination among trusted institutions for primary issuance and shared financial infrastructure. Public blockchains provide neutral settlement layers and liquidity access critical to secondary markets and open financial ecosystems. When combined through hybrid architectures, these models form complementary components of a coherent financial infrastructure.

Hybrid blockchain architectures represent an architectural evolution rather than a transitional compromise. By aligning network types with specific phases of the asset lifecycle, financial enterprises can balance regulatory compliance, operational resilience, and market efficiency within a unified design. Interoperability and compliance-aware integration mechanisms play a central role in enabling this coordination while preserving institutional boundaries and regulatory obligations.

As financial market infrastructure continues to evolve, future research should examine the operational performance, governance dynamics, and risk implications of hybrid deployments at scale. Continued collaboration among industry participants, regulators, and standards bodies will be essential to ensure that hybrid blockchain architectures support innovation while maintaining financial stability. Through disciplined, use-case-driven design, blockchain technologies can be integrated into financial enterprises as durable infrastructure rather than speculative innovation. Future empirical work evaluating operational performance and governance outcomes of hybrid deployments will be critical as these architectures move from pilot programs to systemic financial infrastructure.

Conflict of Interest

The author declares no conflict of interest.

References

[1] B. Charoenwong *et al*., "Blockchain compliance: A framework for evaluating regulatory approaches," Available at SSRN 5368708, 2025.

[2] S. C. Oranburg, "The GENIUS dilemma: Innovation versus antifraud in stablecoin regulation," *Stan. J. Blockchain L. and Pol'y*, vol. 9, p. 99, 2026.

[3] K. Werbach, "The stablecoin toolkit: Financial and market dimensions," Available at SSRN 6123467, 2026.

[4] O. Bodemer, "Blockchain enterprise architecture: Monolith or microservices in the financial industries," Authorea Preprints, 2023.

[5] P. H. B. Correia, M. A. Marques, M. A. Simplicio, L. Ermlivitch, C. C. Miers, and M. A. Pillon, "Comparative analysis of permissioned blockchains: Cosmos, hyperledger fabric, quorum, and XRPL," in P*roc. 2024 IEEE International Conference on Blockchain (Blockchain)*, 2024, pp. 464–469.

[6] M. Mazzoni, A. Corradi, and V. D. Nicola, "Performance evaluation of permissioned blockchains for financial applications: The consensys quorum case study," *Blockchain: Research and Applications*, vol. 3, no. 1, 100026, 2022.

[7] A. Banerjee *et al*., *From Ripples to Waves: The Transformational Power of Tokenizing Assets*, McKinsey and Company: Boston, MA, USA, 2024.

[8] R. Mafrur, "Tokenize everything, but can you sell it? RWA liquidity challenges and the road ahead," arXiv preprint arXiv:2508.11651, 2025.

[9] D. Garofalo, "Strategic decision framework for tokenized funds in commercial banking: A business, technology, and risk perspective," 2025.

[10] J. P. Morgan *et al*., *The Future of Wealth Management: Ultra-Efficient Portfolios of Traditional and Alternative Investments Powered by Tokenization*, JP Morgan Chase & Co. and Apollo Global Management, Inc, 2023.

[11] Institutional DeFi — The next generation of finance? [Online]. Available: https://www.jpmorgan.com/kinexys/documents/Institutional-DeFi-The-Next-Generation-of-Finance.pdf

[12] A. Basu, "Scalable layer 2 and sharding architectures," *Journal of Blockchain Systems and Smart Contracts*, vol. 1, no. 3, 2026.

[13] V. Buterin. (2026). There have recently been some discussions on the ongoing role of L2s in the Ethereum ecosystem, especially in the face of two facts. [Online]. Available: https://x.com/VitalikButerin/status/2018711006394843585

[14] L. Heimbach and J. Milionis, "The early days of the ethereum blob fee," in *Proc. Financial Cryptography and Data Security: 29th International Conference*, 2026, p. 53.

[15] T. Hardjono, A. Lipton, and A. Pentland, "Interoperability challenges in tokenized asset networks," *Transactions of ADIA Lab: Interdisciplinary Advances in Data and Computational Science*, pp. 179–228, 2025.

[16] K. Košťál, D. Morháč, and J. Mečír, "Building interoperability: A decentralized bridge connecting polkadot and cosmos ecosystems," in *Proc. 2025 37th Conference of Open Innovations Association (FRUCT)*, 2025, pp. 136–144.

[17] M. S. Peelam, B. K. Chaurasia, A. K. Sharma, V. Chamola, and B. Sikdar, "Unlocking the potential of interconnected blockchains: A comprehensive study of cosmos blockchain interoperability," *IEEE Access*, vol. 12, pp. 171753–171776, 2024.

[18] P. Sarang and L. Nadkar, *Blockchain Without Barriers: An Authentic Guide to Blockchain Interoperability*, Springer Nature, 2025.

[19] The next-generation monetary and financial system. (2025). [Online]. Available: https://www.bis.org/publ/arpdf/ar2025e3.pdf

[20] Project Promissa: Tokenisation of promissory notes. (2025). [Online]. Available: https://www.bis.org/publ/othp93.pdf

[21] F. Alzhrani, K. Saeedi, and L. Zhao, "Architectural patterns for blockchain systems and application design," *Applied Sciences*, vol. 13, no. 20, 11533, 2023.

[22] B. Shrimali and H. B. Patel, "Blockchain state-of-the-art: Architecture, use cases, consensus, challenges and opportunities," *Journal of King Saud University − Computer and Information Sciences*, vol. 34, no. 9, pp. 6793–6807, 2022.

[23] A. Singh *et al*., *Exploring the Spectrum of Blockchain: Private, Public, Consortium, and Hybrid and their Applications*, Navigating the Blockchain Revolution: Decentralization, Finance, and Beyond. Bentham

Science Publishers, pp. 217–242, 2025.
[24] J. Liu, L. Yan, and D. Wang, "A hybrid blockchain model for trusted data of supply chain finance," *Wireless Personal Communications*, vol. 127, no. 2, 2022.
[25] N. Fikri *et al.*, "A blockchain architecture for trusted sub-ledger operations and financial audit using decentralized microservices," *IEEE Access*, vol. 10, pp. 90873–90886, 2022.
[26] A. Madhavji and J. Xu, "Real-world assets in digital banking: Bridging traditional and digital finance," *Journal of Digital Banking*, vol. 10, no. 1, pp. 54–74, 2025.
[27] R. Priem, "Governance of distributed ledger technology when applied to securities trading: Can a public, permissionless system be the norm?" *Permissionless System be the Norm*, 2024.
[28] K. Patel, "Big data in finance: An architectural overview," Available at SSRN 5280516, 2023.
[29] K. Bear *et al*., *Wholesale Central Bank Digital currencies: Approaches, Implementation Strategies and Use Cases*, 2024.
[30] D. N. Macharia, "Distributed Ledger Technology (DLT) applications in payment, clearing, and settlement systems: A study of blockchain-based payment barriers and potential solutions, and DLT application in central bank payment system functions," University of Huddersfield, 2023.
[31] S. G. Savadatti, S. Krishnamoorthy, and R. Delhibabu, "Survey of Distributed Ledger Technology (DLT) for secure and scalable computing," *IEEE Access*, vol. 13, pp. 8393–8415, 2025.
[32] R. Weerawarna, S. J. Miah, and X. Shao, "Emerging advances of blockchain technology in finance: A content analysis," *Personal and Ubiquitous Computing*, vol. 27, no. 4, pp. 1495–1508, 2023.
[33] T. Schwarze, "Enhancing blockchain security and transparency in the cosmos appchain ecosystem," University of Applied Sciences, 2023.
[34] N. Tovanich *et al*., "SoK: Unified blockchain data structure," in *Proc. 2025 7th International Conference on* Blockchain *Computing and Applications*, 2025, pp. 310–325.
[35] R. Ram, "Deposit tokens: The banking response to stablecoins," Available at SSRN 5378363, 2025.
[36] Designing payment tokens for safety, integrity, interoperability and usability. [Online]. Available: https://www.jpmorgan.com/kinexys/documents/designing-payment-tokens-for-safety-integrity-interoperability-usability.pdf
[37] P. P. Ray, "A survey on model context protocol: Architecture, state-of-the-art, challenges and future directions," Authorea Preprints, 2025.
[38] L. Zhang, "SoK: Stablecoins for digital transformation – Design, metrics, and application with real world asset tokenization as a case study," arXiv preprint arXiv:2508.02403, 2025.
[39] J. Luo, K. Tinn, S. F. Duran, D. Wu, and X. Liu, "Transaction profiling and address role inference in tokenized US treasuries," arXiv preprint arXiv:2507.14808, 2025.
[40] M. Pineda, D. Jabba, and W. N. Bernal, "Blockchain architectures for the digital economy: Trends and opportunities," *Sustainability*, vol. 16, no. 1, p. 442, 2024.
[41] R. Sonmez, F. O. Sönmez, and S. Ahmadisheykhsarmast, "Blockchain in project management: A systematic review of use cases and a design decision framework," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 7, pp. 8433–8447, 2023.
[42] Deposit tokens: A foundation for stable digital money. [Online]. Available: https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2023/feb/oliver-wyman-jp--morgan-deposit-tokens-report-final.pdf
[43] S. V. Hijfte, "Different private and public platforms," *Blockchain Platforms: A Look at the Underbelly of Distributed Platforms*, pp. 261–326, 2025.
[44] H. Koganti, "Understanding Distributed Ledger Technologies (DLT) in financial systems: A comprehensive analysis of architecture, implementation, and impact," *Journal of Engineering and Computer Sciences*, vol. 4, no. 9, pp. 331–347, 2025.
[45] A. A. A. Awamy, N. A. Shaibany, A. Sikora, and D. Welte, "Hybrid consensus mechanisms in blockchain: A comprehensive review," *International Journal of Intelligent Systems*, vol. 1, 5821997, 2025.
[46] D. Duffie, O. Olowookere, and A. Veneris, "Comment in response to the US department of the treasury's advanced notice of proposed rulemaking on the Guiding and Establishing National Innovation for US Stablecoins (GENIUS) act implementation," Available at SSRN 5692624, 2025.